### 1

#### Partisan infrastructure passes now—Biden is key.

Greve 9—7—(staff writer). Joan E Greve. 7 September 2021. “Joe Biden to referee Democrats in brewing battle over $3.5tn budget bill”. The Guardian. <https://amp.theguardian.com/us-news/2021/sep/07/biden-democrats-brewing-battle-budget-bill>. Accessed 9/13/21.

Congress will return from its summer recess later this month, and some Democrats are already gearing up for a political fight – with each other.

Democratic lawmakers are looking to pass their $3.5tn spending package, after the House and the Senate approved the blueprint for the budget bill last month. The ambitious legislation encompasses much of Joe Biden’s economic agenda, including proposals to expand access to affordable childcare, invest in climate-related initiatives and broaden Medicare coverage.

But to get the bill passed, Democrats will first need to reach an agreement on the cost of the legislation. Centrist Democrats, including Senators Kyrsten Sinema and Joe Manchin, have expressed concern about the bill’s $3.5tn price tag, while progressives have indicated they will fiercely oppose any attempt to cut funding in the proposal.

With his entire economic agenda hanging in the balance, Biden will need to convince the two fractious wings of his party to come together and pass a comprehensive spending package. And given Democrats’ extremely narrow majorities in both the House and the Senate, there is virtually no room for error.

#### While popular, the plan costs political capital—trades off.

Carstensen 21—(Fred W. & Vi Miller Chair in Law Emeritus, University of Wisconsin Law School). Peter C. Carstensen. February 2021. “THE “OUGHT” AND “IS LIKELY” OF BIDEN ANTITRUST.” <https://www.concurrences.com/en/review/issues/no-1-2021/on-topic/the-new-us-antitrust-administration-en>.

14. Similarly, despite bipartisan murmurs about competitive issues, the potential in a closely divided Congress that any major initiatives will survive is limited at best. In part the challenge here is how the Biden administration will rank its commitments. If it were to make reform of competition law a major and primary commitment, it would have to trade off other goals, which might include health care reform or increases in the minimum wage. It is likely in this circumstance the new administration, like the Obama administration’s abandonment of the pro-competitive rules proposed under the PSA, would elect to give up stricter competition rules in order to achieve other legislative priorities.

15. Another key to a robust commitment to workable competition is the choice of cabinet and other key administrative positions. Here as well, the early signs are not entirely encouraging. In selecting Tom Vilsack to return as secretary of agriculture, the president has embraced a friend of the large corporate interests dominating agriculture who has spent the last four years in a highly lucrative position advancing their interests. Given the desperate need for pro-competitive rules to implement the PSA and control exploitation of dairy farmers through milk-market orders, the return of Vilsack is not good news. Who will head the FTC and who will be the attorney general and assistant attorney general for antitrust is still unknown, but if those picks are also centrists with strong links to corporate America the hope for robust enforcement of competition law will further attenuate!

16. In sum, this is a pessimistic prognostication for the likely Biden antitrust enforcement agenda. There is much that ought to be done. But this requires a willingness to take major enforcement risks, to invest significant political capital in the legislative process, and to select leaders who are committed to advancing the public interest in fair, efficient and dynamically competitive markets. The early signs are that the new administration will be no more committed to robust competition policy than the Obama administration. Events may force a more vigorous policy—I will cling to that hope as the Biden administration takes shape.

#### The bill solves grid cybersecurity.

Carney 21—(senior policy advisor at Nossaman LLC, former US Representative, former professor of political science at Penn State University). Chris Carney. 8/6/2021. "The US Senate Infrastructure Bill: Securing Our Electrical Grid Through P3s and Grants." <https://www.jdsupra.com/legalnews/the-us-senate-infrastructure-bill-4989100/>.

As we begin to better understand the main components of the Infrastructure Investment and Jobs Act that the US Senate is working to pass this week, it is clear that public-private partnerships ("P3s") are a favored funding mechanism of lawmakers to help offset high costs associated with major infrastructure projects in communities. And while past infrastructure bills have used P3s for more conventional projects, the current bill also calls for P3s to help pay for protecting the US electric grid from cyberattacks. Responding to the increasing number of cyberattacks on our nation’s infrastructure, and given the fragile physical condition of our electrical grid, the Senate included provisions to help state, local and tribal entities harden electrical grids for which they are responsible.

Section 40121, Enhancing Grid Security Through Public-Private Partnerships, calls for not only physical protections of electrical grids, but also for enhancing cyber-resilience. This section seeks to encourage the various federal, state and local regulatory authorities, as well as industry participants to engage in a program that audits and assesses the physical security and cybersecurity of utilities, conducts threat assessments to identify and mitigate vulnerabilities, and provides cybersecurity training to utilities. Further, the section calls for strengthening supply chain security, protecting “defense critical” electrical infrastructure and buttressing against a constant barrage of cyberattacks on the grid. In determining the nature of the partnership arrangement, the size of the utility and the area served will be considered, with priority going to utilities with fewer available resources.

Section 40122 compliments the previous section as it seeks to incentivize testing of cybersecurity products meant to be used in the energy sector, including SCADA systems, and to find ways to mitigate any vulnerabilities identified by the testing. Intended as a voluntary program, utilities would be offered technical assistance and databases of vulnerabilities and best practices would be created. Section 40123 incentivizes investment in advanced cybersecurity technology to strengthen the security and resiliency of grid systems through rate adjustments that would be studied and approved by the Secretary of Energy and other relevant Commissions, Councils and Associations.

Lastly, Section 40124, a long sought-after package of cybersecurity grants for state, local and tribal entities is included in the bill. This section adds language that would enable state, local and tribal bodies to apply for funds to upgrade aging computer equipment and software, particularly related to utilities, as they face growing threats of ransomware, denial of service and other cyberattacks. However, under Section 40126, cybersecurity grants may be tied to meeting various security standards established by the Secretary of Homeland Security, and/or submission of a cybersecurity plan by a grant applicant that shows “maturity” in understanding the cyber threat they face and a sophisticated approach to utilizing the grant.

While the final outcome of the Infrastructure Investment and Jobs Act may still be weeks or months away, inclusion of these provisions not only demonstrates a positive step forward for the application of federal P3s and grants generally, they also show that Congress recognizes the seriousness of the cyber threats our electrical grids face. Hopefully, through judicious application of both public-private partnerships and grants, the nation can quickly secure its infrastructure from cyberattacks.

#### Goes nuclear.

Klare 19—(professor emeritus of peace and world security studies at Hampshire College). Michael Klare. November 2019. “Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation.” Arms Control Association. <https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation>.

Yet another pathway to escalation could arise from a cascading series of cyberstrikes and counterstrikes against vital national infrastructure rather than on military targets. All major powers, along with Iran and North Korea, have developed and deployed cyberweapons designed to disrupt and destroy major elements of an adversary’s key economic systems, such as power grids, financial systems, and transportation networks. As noted, Russia has infiltrated the U.S. electrical grid, and it is widely believed that the United States has done the same in Russia.12 The Pentagon has also devised a plan known as “Nitro Zeus,” intended to immobilize the entire Iranian economy and so force it to capitulate to U.S. demands or, if that approach failed, to pave the way for a crippling air and missile attack.13

The danger here is that economic attacks of this sort, if undertaken during a period of tension and crisis, could lead to an escalating series of tit-for-tat attacks against ever more vital elements of an adversary’s critical infrastructure, producing widespread chaos and harm and eventually leading one side to initiate kinetic attacks on critical military targets, risking the slippery slope to nuclear conflict. For example, a Russian cyberattack on the U.S. power grid could trigger U.S. attacks on Russian energy and financial systems, causing widespread disorder in both countries and generating an impulse for even more devastating attacks. At some point, such attacks “could lead to major conflict and possibly nuclear war.”14

### 2

#### The DOJ has prioritized combatting COVID related fraud—key to healthcare cybersecurity

Anna Dykema et. al 21, Anna graduated Order of the Coif from University of Denver Sturm College of Law, Tom McSorley, advises clients on the intersection of law, technology, national security, and foreign policy, Christian Sheehan, law clerk for the Honorable D. Michael Fisher on the US Court of Appeals for the Third Circuit, “DOJ Gives the First Glimpse into FCA Enforcement Priorities Under the Biden Administration—Some Expected, Others Less So”, <https://www.arnoldporter.com/en/perspectives/blogs/fca-qui-notes/posts/2021/03/doj-gives-glimpse-into-fca-enforcement-priorities>, March 4th, 2021

In a recent speech, Department of Justice (DOJ) Acting Assistant Attorney General Brian Boynton provided the first glimpse into DOJ's False Claims Act (FCA) enforcement priorities under the Biden Administration. While much of the speech predictably focused on pandemic-related fraud and opioid enforcement efforts, a few measures announced by the AAG were less expected. In particular, AAG Boynton highlighted DOJ's increased focus on violations of cybersecurity requirements and made clear that FY 2020's increase in cases brought directly by DOJ is a trend we should expect to continue. Unsurprisingly, pandemic and opioid-related fraud top DOJ's priority list. The AAG anticipated that the FCA will be a primary enforcement vehicle for what he called the "inevitable fraud schemes" stemming from COVID-19 relief programs, including the CARES Act and loans through the Paycheck Protection Program (PPP). As we previously reported, just last month, DOJ announced the first civil settlement involving PPP-related fraud allegations—likely the first of many. The FCA will also continue to be one of the primary enforcement tools to hold companies liable for improperly promoting the sale and use of opioids. Opioid-related enforcement produced a blockbuster recovery earlier this year when DOJ announced in October 2020 a $3 billion-plus FCA settlement with Purdue Pharma (part of an $8 billion global criminal and civil settlement). AAG Boynton also explained that we are likely to continue to see more cases brought directly by DOJ. DOJ's FY 2020 stats showed that DOJ filed more direct cases last year than ever before. We now have a better understanding of why that is. AAG Boynton stated that DOJ is looking to "expand its own efforts to identify potential fraudsters" by leveraging its "sophisticated data analytics" system. This is not the first instance of DOJ aiming to enhance its data analytics. You may recall that last year, DOJ announced that it was initiating a data-driven approach to PPP enforcement and investigation. AAG Boynton also explained that DOJ is using data analytics "to identify patterns across different types of health care providers – giving us a way to identify trends and extreme outliers." He said that the data allows DOJ to "see where the highest risk physicians are located in each state and federal district, and how much they are costing" the government. Expect more to come on this front. Also noteworthy from the AAG's speech was DOJ's heightened focus on using the FCA to police compliance with cybersecurity requirements. DOJ has already started to lay the groundwork for enforcement in this area. In the much-discussed decision of United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc., No. 15-cv-2245, 2019 WL 2024595 (E.D. Ca. May 8, 2019), the court upheld the government's enforcement action against a firm that represented it was in compliance with the cybersecurity standards in its Department of Defense (DoD) contract when it allegedly knew these representations were inaccurate. Subsequently, in July 2019, another contractor agreed to an $8.6 million settlement to resolve allegations that it sold cybersecurity-vulnerable software to federal, state, and local government agencies in violation of contractual requirements. This was the first reported settlement based on FCA allegations related to cybersecurity noncompliance—but it is unlikely to be the last.

#### But resource constraints limit cases--the plan trades-off

Alex Kantrowitz 20, Founder at Big Technology | Author of ALWAYS DAY ONE: How The Tech Titans Plan To Stay On Top Forever, “It’s Ridiculous.’ Underfunded FTC and DOJ Can’t Keep Fighting the Tech Giants Like This”, <https://bigtechnology.substack.com/p/its-ridiculous-underfunded-us-regulators>, September 17th, 2020

As politicians, the press, and the public scrutinize the tech giants and grow wary of their power, the most important organizations tasked with restraining them — the U.S. regulatory agencies — aren’t getting enough funding to do the job. “The agencies are severely resource-constrained,” Michael Kades, an-ex FTC trial lawyer who spent 11 years at the agency, told Big Technology. The Federal Trade Commission and Department of Justice’s antitrust division have a combined annual budget below what Facebook makes in three days. The FTC runs on less than $350 million per year, the DOJ’s antitrust division on less than $200 million. Facebook made $18 billion last quarter alone. The funding disparity between the tech giants and their regulators leads to an unbalanced fight, current and ex-staffers said: The agencies can’t investigate the tech giants to the extent they’d like. They might shy away from complex cases fearing a resource-draining battle. And when they investigate the tech giants, they often see former colleagues with intricate knowledge of their strategy and ability to act (or lack thereof) representing these companies. Without significant budget increases, the tech giants may well continue to act unrestrained with little fear of repercussions. “DOJ is under-resourced, FTC it’s ridiculous,” one ex DOJ-staffer told Big Technology. This doesn’t mean these agencies are entirely hamstrung; they can typically marshall the resources to bring a clear-cut case. “They want to win,” one ex-FTC official said. “If it's really egregious, and they find that in discovery, the attorneys are going to put a case together and go after it.” But when you can only take up a limited number of cases due to resource constraints, things inevitably slip through. “When I was there, the privacy wing had maybe 50 people, and that's probably generous. That's lawyers, support staff, everyone,” Justin Brookman, the former policy director at the FTC’s office of technology research and investigation, told Big Technology. “If they were to bring a case, that would tie up half the resources of the group. And they had two litigations ongoing and that took up most of everyone's time.” The agency’s budget has barely increased since Brookman left in 2017, while the tech giants have added trillions of dollars to their market caps. Inside the FTC and DOJ, employees are aware of the tech giants’ ability to fight, and the corporations’ budgets tend to live inside their heads. “Facebook will have the ability to raise every single issue, if they want to,” Kades said. “It doesn't have to be a winner, doesn't have to be close to winner. If they wanted to take this position in litigation, they can make every procedural maneuver difficult, they can not cooperate on discovery, they can fight on scheduling, they don't have to win even half of those, but it would just suck up resources.” The ability to do this, not even the action itself, can impact regulators’ thinking. Agency staffers are typically mission-driven and knowingly work for salaries below private-sector rates, but the resource-rich tech giants are now poaching directly from agencies at a rate remarkable even for Washington’s revolving door between the private and public sector.

#### Cyberattacks collapse the healthcare sector

Tracy Batsford 21, Owner and President at Communication Anglaise, 15 years’ experience in sales and marketing in the high-tech sector, “How Do Cyber Attacks Happen in Hospitals and Healthcare Clinics?”, <https://hellohealth.com/blog/how-do-cyber-attacks-happen-in-hospitals-and-healthcare-clinics/>, April 15th, 2021

As healthcare institutions grapple with the fight against COVID-19, another fight is also far from over: cyberattacks against hospitals and clinics. According to Cybersecurity Ventures, the healthcare industry, which is a $1.2 trillion sector, will fall victim to two to three times more cyberattacks in 2021 than the average numbers for other industries. Even more worrisome: Black Book Market Research has indicated that: “more than 93 percent of healthcare organizations have experienced a data breach over the past three years, and 57 percent have had more than five data breaches during the same time frame.” Threat analysts from cybersecurity company Emsisoft Ltd. told the Wall Street Journal that medical testing laboratories, medical device manufacturers and carriers of critical medical supplies are also facing a dramatic increase in threats to their cybersecurity. The dramatic increase in attacks compromises both patient safety and the public’s trust in the healthcare sector. But the questions remain: why do cyberattacks happen in hospitals and healthcare clinics? What are the strategies that can help them mitigate the devastating impact of a breach. Why Should Hospitals Care About Cybersecurity? Threats to hospitals’ cybersecurity cost the healthcare sector millions each year. A case in point: Universal Health Services, one of the largest hospital chains in the United States, was attacked late last September, which ended up costing the company $67 million last year. Due to ransomware, which shut down computer systems for medical records, pharmacies and labs across 250 facilities, ambulances had to be diverted to other hospitals and critical surgeries ended up being postponed as IT experts raced to restore infrastructure and even connected medical devices. Unfortunately, cases like Universal Health Services are far too common. Cyberattacks costs hospitals millions each year In a recent IBM report, healthcare clinics and hospitals incur the highest average security breach cost of any industry. In fact, cyberattacks can cost one institution US $7.13 million per incident—and even higher. Take Sky Lakes Medical Center, located in Oregon. In October 2020, the center was dealing with a massive surge in COVID-19 hospitalizations when hackers sent malware to the institution’s network, leaving staff without access to medical records and equipment. One month after the attack, the associated costs of building the network with new servers and computers as well as lost revenue from the incident was estimated at US $10 million. Comparitech analysts estimate that ransomware attacks on US healthcare organizations cost them US $20B in 2020 alone. The company indicates that there has been an increasing trend in double extortion attempts in which cybercriminals not only deny access with a ransom message but also call patients with proof of the data collected. This new trend is often forcing hospitals and clinics to pay out the ransom amounts, which incentivizes future cyberattacks. Patients Put at Risk The barrage of cyberattacks on healthcare organizations is not just about their bottom lines. A 2020 Cybersecurity Survey from the Healthcare Information and Management Systems Society (HIMSS) offered somber news for hospitals and clinics that didn’t invest substantially more in their cybersecurity: “Historically, hackers have threatened the confidentiality of medical information through data breaches where they obtain Social Security numbers or financial data. But if hackers threaten the integrity of medical data, such as by changing laboratory values or hacking a remote medical device, that could pose a very real danger to patients,” said Rod Piechowski, health IT expert and Vice-President of Thought Advisory at the HIMSS, during an interview about the study. Even more disturbing is how sophisticated cyberattacks can become, doing more harm on patients. For example, in a bid to raise awareness in cybersecurity weaknesses in medical equipment and devices, researchers in Israel were able to create a malware capable of adding or removing tumors in CT and MRI scans—tricking radiologists into providing false diagnoses. In 87% of the cases in which the malware removed cancerous modules, doctors concluded very sick patients were actually healthy. The Israeli research team said that the malware could be used for all types of health issues, including brain tumors, heart disease, blood clots, spinal injuries, and more. One cyberattack alone can cost a healthcare organization at least US $7.13 million. Why is The Healthcare Sector a Primary Target for Cyber-Attacks? The healthcare sector is notorious for being a target for cyberattacks. Many hospitals and clinics rely on outdated systems and infrastructure with minimal resilience to cyberattacks. On the other side of the spectrum, more modern healthcare facilities are increasingly reliant on networked digital infrastructure as well as medical equipment and devices that use IoT sensors to connect them to centralized networks. While electronic data sharing and virtual services can facilitate and accelerate patient care, they are still vulnerable to security breaches that affect how they operate. In these cases, cyberattacks can not only access the equipment’s configurations and settings—but also the hospital networks to which they are connected. Another reason healthcare organizations are a goldmine for cybercriminals is their financial resources. In privatized healthcare networks, hospitals and clinics often have substantial financial resources to actually pay ransomware, for example. In the public sector, the situation can be the complete opposite; with lack of financial resources, hospitals and clinics rely on legacy technology that cannot withstand attacks. Furthermore, healthcare organizations have been slow to adopt cybersecurity best practices and technologies, according to the Harvard Business Review. In IBM’s aforementioned survey, just 23% of hospitals and clinics have fully deployed security automation tools. The HIMSS survey showed that healthcare organizations dedicated only 6% or less of their IT budgets to cybersecurity, making them very much prone to hackers. Cybercriminals also don’t just “attack” IT infrastructure. They also target healthcare professionals. This approach is three-pronged. For one, human error accounts for 95% of security breaches. This means that hospital or clinic employees’ unintentional actions, such as downloading a malware-infected attachment or failing to use a strong password, can pave the way for a breach. This situation is exacerbated by the fact that many healthcare professionals in human resources, accounts payable and other departments are working from home. As Jeff Brown, CEO of the cybersecurity company Open Systems, said in a recent interview with Silicon Republic: Cybercriminals “are currently taking advantage of the thousands of healthcare workers in human resources, accounts payable and other departments who are working from home due to the pandemic.” They are also targeting healthcare professionals conducting telemedicine at home. These remote employees all have to connect to applications and data to carry out their day-to-day tasks. Without the proper cybersecurity measures and training in place, hackers can easily penetrate entire hospital networks—either to steal financial, employee or patient data, or hijack accounts for ransom.

#### Extinction

Royi Barnea et. al 20, Barnea is a Business Development Manager and Sales Expert with more than 20 years of experience in the Israeli and US Market, Yossi Weiss , Prof, Head of Department of Health Sciences School, Prof. Joshua Shemer chairs the Assuta Medical Centers network in Israel, “Health: an essential component of national resilience”, <https://www.joghr.org/article/14134-health-an-essential-component-of-national-resilience>, August 17th, 2020

The term “national resilience” originally referred only to a country’s military capacity, but was later expanded to include political-psychological aspects.5 According to Friedland, “national resilience” is the ability of a society to withstand adversities and crises, such as natural disasters or national security events (wars or terror attacks) in diverse realms by implementing changes and adaptations without harming society’s core values and institutions.6,7 Kimhi and Eshel have suggested that community resilience and national resilience are overlapping expressions of public resilience that provides its members with social identity, a sense of belonging and security.5 Since the beginning of the second millennium, there has been a growth in the number of policy documents relating to national resilience published by various organizations and countries (Table 1). These definitions imply that national resilience is usually perceived in terms of well-being and sustainability as well as in terms of risk management which has grown from the need of countries to deal with security threats such as terrorism, economic crises (e.g. the 2008 global economic crisis), and more prevalent natural disasters due to climate change. In 2011, the OECD started a program to measure well-being in various countries. Well-being measures include household, income, employment, community, education, environment, civic obligations, health, satisfaction and life, security and life-work balance. In addition to measuring well-being, the OECD has published an agenda for the advancement of sustainability in the various countries – the ‘2030 Agenda for Changing the World’. Evaluation of national policies for strength, well-being and sustainability of the 38 OECD countries as well as India and China has shown that determinants of resilience included first and foremost health (100% of countries), the economy (in 88% of countries), the environment (68%, including, agriculture, forestry, fishing, and conservation of natural resources), personal security (64%), quality of employment (64%), industry, infrastructure and accommodation (52%), civil and government involvement (52%), information, communication and innovation (48%), education and skills (44%), energy (40%), transportation and logistics (24%), plans for land utilization (12%) and leisure, culture and community (12%). In Israel, following the financial crisis of 2008, a government resolution was put forth to develop indicators and metrics of well-being, sustainability and national resilience that would complement the national accounting system and the gross domestic product. A team of professionals from the Central Bureau of Statistics, the Prime Minister’s Office, the National Economic Council and the Ministry for Environmental Protection established a list of 72 quality-of-life metrics in nine areas: income and capital, civil involvement and government, employment and balance of work and leisure, education and skills, environment, health, personal and social welfare, personal security, and infrastructure and housing.12 The metrics are published annually by the government statistician in order to help and formulate up-to-date policies. Health as a determinant of national resilience A health component is included in all three levels of resilience suggesting that health is an important determinant of resilience at all societal levels. Bonanno et al. defined “personal resilience” as the ability of the individual to function in a stable manner after traumatic events and to maintain healthy functioning over time.12 Community resilience requires the community’s constant and evolving ability to respond to its vulnerability and develop capabilities that help the community (1) prevent, meet and reduce the stress of a health incident; (2) to recover in a manner that will restore the community to a state of independence and at least the same level of health and social functioning after a health incident; (3) using knowledge from past experience to strengthen the community’s ability to withstand the next health incident.13 Thus, community resilience includes the protection of human life, health, economy and preparedness of infrastructures and the environment for coping. There are those who argue that community resilience is also related to perceived social support, to the strength of social connections, and to the physical and mental health of the public.1 According to Wulff et al., community resilience stems from good health and strong health systems, improved health status of populations, and the ability to maintain a healthy physical and mental state of individuals and communities and to deal with major physical and mental changes.14 Consequently, health systems can be regarded as the key to promoting community health resilience. In line with this premise, the WHO contends that the main factor that helps to create strength and resilience is a strong health system that provides a comprehensive response to all citizens. Health resilience is established by improved health status, strong health systems, good health outcomes, and is measured in the ability to preserve the physical, mental and social condition of the community and detail it in the course of large-scale changes.15 The WHO has identified six building blocks to strengthen health systems and increase resilience by improving health outcomes and accessibility as well as the health needs of the population, managing the individual’s economic and social risks, and improving the efficiency of the system. These building blocks relate to public and private resources and include health services, personnel, information, access to medical equipment, vaccines and the quality and safety of technology, finance and coverage, governance and leadership.15 Strengthening the health system by improving health outcomes, such as health indicators, response to health needs, protection from economic and social risks (insurance coverage) and efficiency of the system should increase the strength and resilience of the community and the nation.

### 3

#### The USFG should implement HR 676: The Expanded and Improved Medicare for All Act.

#### HR 676 provides for basic health care for all Americans:

Dennis Kucinich, 3-22-2017, (former Chair of the Congressional Progressive Caucus, represented Ohio's 10th District from 1997 to 2013) "Saving Obamacare Is Not Enough—We Need Medicare for All," Nation, <https://www.thenation.com/article/saving-obamacare-is-not-enough-we-need-medicare-for-all/> ach

Here is what the for-profit insurance system brings: Rising premiums and co-pays. Diminishing coverage. More government subsidy of private insurers. Rising costs for prescription drugs. More people going bankrupt because of hospital bills. More people losing their homes because of hospital bills. More seniors forced into poverty, losing everything they worked for their entire lives. This is not about Democrats vs. Republicans, liberals vs. conservatives, left vs. right. This is about life vs. death. This is about whether we, as Americans, can recognize a common interest in using the vast resources of our nation to insure the health of our people. Heath spending approaches nearly 18 percent of the $20 trillion GDP. Nearly a trillion dollars of that amount goes for corporate profits, stock options, executive salaries, advertising, marketing, and the cost of paperwork. If we took all the money that people and the government are presently paying into the for-profit system and applied it to care for people in a not-for-profit system, we could provide for basic health care for all Americans, including prescription drugs, vision care, dental care, mental-health care, and long-term care. That is what HR 676, Medicare for All, was all about. Medicare for All is an idea whose time has come. Let’s make all Americans healthy and wealthy. Let’s lift up all of our families, save our homes, and help our businesses and industries. Let’s join every other industrialized nation in the world and offer health care to all of our people.

#### Single-payer health care is necessary to solve for pandemics

**Kahn 17** [Laura Kahn is the author of One Health and the Politics of Antimicrobial Resistance, Why access to health care is a national security issue, Bulletin of the Atomic Scientists, June 5, 2017, <http://thebulletin.org/why-access-health-care-national-security-issue10819>] BJ

The Canadian government’s response had its glitches—primarily in the form of poor political leadership. Mel Lastman, the mayor of Toronto and a former furniture salesman, became angry when the World Health Organization (WHO) issued a travel advisory against his city. He railed against the WHO’s decision on television, revealing his complete lack of knowledge about either the organization or public health in general. As a result of Lastman’s poor leadership, he was ultimately relegated to a secondary role as the deputy mayor took his place. Lastman’s credibility and legitimacy never recovered from the SARS outbreak. Likewise, US leaders will be judged by how they handle a bioterrorist attack or pandemic. Unlike Canada, America’s piecemeal healthcare and public health systems are inherently less able to handle such crises. The Affordable Care Act helped fill in the gaps, but really, the only way to prepare for the eventuality of pandemics or bioterrorist attacks is with a single-payer government-run system that covers everyone. The United States might consider modeling its health care system after the one in Israel, a country that, given longstanding threats, takes every terrorist risk very seriously. In 1994, it established universal health coverage for all citizens. The country’s Ministry of Health monitors and promotes public health, oversees the operations of the nation’s hospitals, and sets healthcare priorities. As a result, Israel’s public health, emergency response, and hospital systems are state-of-the-art, highly efficient, and coordinated—a necessity when responding to terrorist attacks. The preamble to the US Constitution states the goals to “provide for the common defense” and “promote the general Welfare.” The US government won’t fulfill either of these duties if it fails to protect its citizens against pandemics and bioterrorism. The mandate requires a robust public health infrastructure and a universal healthcare system that covers all Americans. The Trump Administration and Congressional Republicans threaten to undermine this essential function of government, unnecessarily jeopardizing American lives..

### 4

The fifty states and relevant subnational entities should lower the transaction threshold for premerger notifications and automatic review of Mergers.

#### State action is coordinated, well-resourced, and solves.

Arteaga ’21 [Juan and Jordan Ludwig; January 28; former Deputy Assistant Attorney General for the U.S. Department of Justice’s Antitrust Division, J.D. from Columbia Law School; partner in the Antitrust and Competition Group at Crowell and Moring firm, J.D. from Loyola Law School; Global Competition Review, “The Role of US State Antitrust Enforcement,” <https://globalcompetitionreview.com/guide/private-litigation-guide/second-edition/article/the-role-of-us-state-antitrust-enforcement>]

In the United States, competition laws have been implemented and enforced through a dual system where the state and federal governments play distinct, yet complementary, roles in regulating the competitive process. While the Department of Justice (DOJ) Antitrust Division and Federal Trade Commission (FTC) are widely viewed as the stewards of US antitrust laws, state attorneys general have long played an important, albeit varying, role within the United States’ antitrust enforcement regime. This has been especially true during the past 30 years because state attorneys general have become much more effective at coordinating their antitrust enforcement efforts to ensure that they have a meaningful seat at the table in any actions brought jointly with their federal counterparts or are able to bring their own actions when the DOJ and FTC decide not to do so. Prior to the enactment of the first federal antitrust law – the Sherman Act – in 1890, state antitrust enforcement was quite robust in the United States because at least 26 states had already enacted some form of antitrust prohibition.[[2]](https://globalcompetitionreview.com/guide/private-litigation-guide/second-edition/article/the-role-of-us-state-antitrust-enforcement#footnote-126) In addition, state enforcers had often used general corporation law and common law restraint of trade principles to regulate anticompetitive business practices and transactions.[[3]](https://globalcompetitionreview.com/guide/private-litigation-guide/second-edition/article/the-role-of-us-state-antitrust-enforcement#footnote-125) This well-established state antitrust enforcement infrastructure – coupled with the fact that the Antitrust Division and FTC had only recently been created – permitted state attorneys general to continue playing a leading enforcement role for the first 30 years after the Sherman Act’s passage.[[4]](https://globalcompetitionreview.com/guide/private-litigation-guide/second-edition/article/the-role-of-us-state-antitrust-enforcement#footnote-124) Indeed, state attorneys general successfully prosecuted a number of the most consequential antitrust enforcement actions during this period.[[5]](https://globalcompetitionreview.com/guide/private-litigation-guide/second-edition/article/the-role-of-us-state-antitrust-enforcement#footnote-123) In the early 1920s, however, state antitrust enforcers began playing a less prominent role because ‘the national dimension of the most important trusts, . . . as well as their ability to restructure in order to evade problematic state laws’, made clear that the federal government needed to step forward in order to adequately protect consumers and the competitive process.[[6]](https://globalcompetitionreview.com/guide/private-litigation-guide/second-edition/article/the-role-of-us-state-antitrust-enforcement#footnote-122) As a result, the DOJ and FTC – whose national jurisdiction and greater resources enabled them to tackle the most pressing competition issues of the time – displaced state attorneys general as the primary source of government antitrust enforcement within the United States.[[7]](https://globalcompetitionreview.com/guide/private-litigation-guide/second-edition/article/the-role-of-us-state-antitrust-enforcement#footnote-121) This largely remained true until the mid-1970s when Congress, in response to the DOJ and FTC’s perceived inactivity, passed two laws that expanded the authority of state attorneys general to enforce the federal antitrust laws and provided them with financial resources to do so.[[8]](https://globalcompetitionreview.com/guide/private-litigation-guide/second-edition/article/the-role-of-us-state-antitrust-enforcement#footnote-120) In 1976, Congress passed the Hart-Scott-Rodino Antitrust Improvement Act, which, among other things, authorized state attorneys general to bring parens patriae suits (i.e., legal actions brought on behalf of natural persons residing within their states) seeking monetary (treble damages) and injunctive relief for Sherman Act violations.[[9]](https://globalcompetitionreview.com/guide/private-litigation-guide/second-edition/article/the-role-of-us-state-antitrust-enforcement#footnote-119) Congress also passed the Crime Control Act of 1976, which, among other things, provided state attorneys general with tens of millions in federal grants as ‘seed money’ for the creation of antitrust bureaus within their offices.[[10]](https://globalcompetitionreview.com/guide/private-litigation-guide/second-edition/article/the-role-of-us-state-antitrust-enforcement#footnote-118) These laws had their intended effect of reinvigorating state antitrust enforcement. During the 1980s, for example, state attorneys general once again emerged as vigorous antitrust enforcers, especially with respect to the prosecution of resale price maintenance practices and other vertical restraints.[[11]](https://globalcompetitionreview.com/guide/private-litigation-guide/second-edition/article/the-role-of-us-state-antitrust-enforcement#footnote-117) The rise in the level and prominence of state antitrust enforcement during this period was largely due to a perceived enforcement void at the federal level, where the DOJ and FTC had mostly limited their focus to ‘prohibiting cartels and large horizontal mergers’.[[12]](https://globalcompetitionreview.com/guide/private-litigation-guide/second-edition/article/the-role-of-us-state-antitrust-enforcement#footnote-116) No longer content with ceding antitrust enforcement to federal enforcers, state attorneys general expanded their antitrust dockets from prosecuting purely ‘local matters, such as bid-rigging on state contracts’, to actively investigating and litigating matters with multistate and national implications.[[13]](https://globalcompetitionreview.com/guide/private-litigation-guide/second-edition/article/the-role-of-us-state-antitrust-enforcement#footnote-115) To help ensure that they had a larger seat at the antitrust enforcement table, state attorneys general also increased the coordination of their enforcement efforts and competition advocacy through organizations such as the National Association of Attorneys General (NAAG), which created a Multistate Antitrust Task Force and issued state Vertical Restraints and Horizontal Merger Guidelines during this period.[[14]](https://globalcompetitionreview.com/guide/private-litigation-guide/second-edition/article/the-role-of-us-state-antitrust-enforcement#footnote-114)

### Case

#### Extinction outweighs

Bostrom 12 – Director of the Future of Humanity Institute at Oxford

(Nick, “We're Underestimating the Risk of Human Extinction,” interview with Ross Andersen, freelance writer in D.C., 3-6-12, http://www.theatlantic.com/technology/archive/2012/03/were-underestimating-the-risk-of-human-extinction/253821/)

Some have argued that we ought to be directing our resources toward humanity's existing problems, rather than future existential risks, because many of the latter are highly improbable. You have responded by suggesting that existential risk mitigation may in fact be a dominant moral priority over the alleviation of present suffering. Can you explain why? Bostrom: Well suppose you have a moral view that counts future people as being worth as much as present people. You might say that fundamentally it doesn't matter whether someone exists at the current time or at some future time, just as many people think that from a fundamental moral point of view, it doesn't matter where somebody is spatially---somebody isn't automatically worth less because you move them to the moon or to Africa or something. A human life is a human life. If you have that moral point of view that future generations matter in proportion to their population numbers, then you get this very stark implication that existential risk mitigation has a much higher utility than pretty much anything else that you could do. There are so many people that could come into existence in the future if humanity survives this critical period of time---we might live for billions of years, our descendants might colonize billions of solar systems, and there could be billions and billions times more people than exist currently. Therefore, even a very small reduction in the probability of realizing this enormous good will tend to outweigh even immense benefits like eliminating poverty or curing malaria, which would be tremendous under ordinary standards.

#### Debating existential risks is the most important thing debate can do—leads to civic engagement and awareness.

Javorksy 18—Emilia, MD, MPH is a physician-scientist focused on the invention, development and commercialization of new medical therapies. She also leads an Artificial Intelligence in Medicine initiative with The Future Society (TFS) at the Harvard Kennedy School of Government, and is helping to launch a TFS initiative focused on the role of creativity in shaping a positive future. She was a 2012-13 Fulbright-Schuman Scholar to the European Union, is a TEDx speaker, a member of the World Economic Forum's Global Shaper community, and was honored as part of the Forbes 30 Under 30 Class of 2017 in Healthcare., 1-15-2018, ("Why Human Extinction Needs a Marketing Department," <https://www.xconomy.com/boston/2018/01/15/why-human-extinction-needs-a-marketing-department/>)

Experts at Oxford University and elsewhere have estimated that the risk of a global human extinction event this century—or at least of an event that wipes out 10 percent or more of the world’s population— is around 1 in 10. The most probable culprits sending us the way of the dinosaur are mostly anthropogenic risks, meaning those created by humans. These include climate change, nuclear disaster, and more emerging risks such as artificial intelligence gone wrong (by accident or nefarious intent) and bioterrorism. A recent search of the scientific literature through ScienceDirect for “human extinction” returned a demoralizing 157 results, compared to the 1,627 for “dung beetle.” I don’t know about you, but this concerns me. Why is there so little research and action on existential risks (risks capable of rendering humanity extinct)? A big part of the problem is a lack of awareness about the real threats we face and what can be done about them. When asked to estimate the chance of an extinction event in the next 50 years, U.S. adults in surveys reported chances ranging from 1 in 10 million to 1 in 100, certainly not 10 percent. The awareness and engagement issues extend to the academic community as well, where a key bottleneck is a lack of talented people studying existential risks. Developing viable risk mitigation strategies will require widespread civic engagement and concerted research efforts. Consequently, there is an urgent need to improve the communication of the magnitude and importance of existential risks. The first step is getting an audience to pay attention to this issue.

#### High magnitude impacts outweigh, even with low probability.

Bostrom 13—Nick, Philosopher and professor (Oxford), Ph.D. (LSOE), director of The Future of Humanity Institute and the Programme on the Impacts of Future Technology, of course, he’s also the inaugural recipient of “The Eugene R. Gannon Award for the Continued Pursuit of Human Advancement,” “Existential Risk Prevention as Global Priority,” Global Policy, Vol 4, Issue 1, <http://www.existential-risk.org/concept.html>

The maxipok rule 1.1. Existential risk and uncertainty An existential risk is one that threatens the premature extinction of Earth-originating intelligent life or the permanent and drastic destruction of its potential for desirable future development (Bostrom 2002). Although it is often difficult to assess the probability of existential risks, there are many reasons to suppose that the total such risk confronting humanity over the next few centuries is significant. Estimates of 10-20% total existential risk in this century are fairly typical among those who have examined the issue, though inevitably such estimates rely heavily on subjective judgment.1 The most reasonable estimate might be substantially higher or lower. But perhaps the strongest reason for judging the total existential risk within the next few centuries to be significant is the extreme magnitude of the values at stake. Even a small probability of existential catastrophe could be highly practically significant (Bostrom 2003; Matheny 2007; Posner 2004; Weitzman 2009). Humanity has survived what we might call natural existential risks for hundreds of thousands of years; thus it is prima facie unlikely that any of them will do us in within the next hundred.2 This conclusion is buttressed when we analyze specific risks from nature, such as asteroid impacts, supervolcanic eruptions, earthquakes, gamma-ray bursts, and so forth: Empirical impact distributions and scientific models suggest that the likelihood of extinction because of these kinds of risk is extremely small on a time scale of a century or so.3 In contrast, our species is introducing entirely new kinds of existential risk — threats we have no track record of surviving. Our longevity as a species therefore offers no strong prior grounds for confident optimism. Consideration of specific existential-risk scenarios bears out the suspicion that the great bulk of existential risk in the foreseeable future consists of anthropogenic existential risks — that is, those arising from human activity. In particular, most of the biggest existential risks seem to be linked to potential future technological breakthroughs that may radically expand our ability to manipulate the external world or our own biology. As our powers expand, so will the scale of their potential consequences — intended and unintended, positive and negative. For example, there appear to be significant existential risks in some of the advanced forms of biotechnology, molecular nanotechnology, and machine intelligence that might be developed in the decades ahead. The bulk of existential risk over the next century may thus reside in rather speculative scenarios to which we cannot assign precise probabilities through any rigorous statistical or scientific method. But the fact that the probability of some risk is difficult to quantify does not imply that the risk is negligible. Probability can be understood in different senses. Most relevant here is the epistemic sense in which probability is construed as (something like) the credence that an ideally reasonable observer should assign to the risk's materializing based on currently available evidence.4 If something cannot presently be known to be objectively safe, it is risky at least in the subjective sense relevant to decision making. An empty cave is unsafe in just this sense if you cannot tell whether or not it is home to a hungry lion. It would be rational for you to avoid the cave if you reasonably judge that the expected harm of entry outweighs the expected benefit. The uncertainty and error-proneness of our first-order assessments of risk is itself something we must factor into our all-things-considered probability assignments. This factor often dominates in low-probability, high-consequence risks — especially those involving poorly understood natural phenomena, complex social dynamics, or new technology, or that are difficult to assess for other reasons. Suppose that some scientific analysis A indicates that some catastrophe X has an extremely small probability P(X) of occurring. Then the probability that A has some hidden crucial flaw may easily be much greater than P(X).5 Furthermore, the conditional probability of X given that A is crucially flawed, P(X|¬A), may be fairly high. We may then find that most of the risk of X resides in the uncertainty of our scientific assessment that P(X) was small (figure 1) (Ord, Hillerbrand and Sandberg 2010).

#### Death outweighs – ontologically destroys the subject

Paterson 03 – Department of Philosophy, Providence College, Rhode Island

(Craig, “A Life Not Worth Living?”, Studies in Christian Ethics, http://sce.sagepub.com)

Contrary to those accounts, I would argue that it is death per se that is really the objective evil for us, not because it deprives us of a prospective future of overall good judged better than the alter- native of non-being. It cannot be about harm to a former person who has ceased to exist, for no person actually suffers from the sub-sequent non-participation. Rather, death in itself is an evil to us because it ontologically destroys the current existent subject — it is the ultimate in metaphysical lightening strikes.80 The evil of death is truly an ontological evil borne by the person who already exists, independently of calculations about better or worse possible lives. Such an evil need not be consciously experienced in order to be an evil for the kind of being a human person is. Death is an evil because of the change in kind it brings about, a change that is destructive of the type of entity that we essentially are. Anything, whether caused naturally or caused by human intervention (intentional or unintentional) that drastically interferes in the process of maintaining the person in existence is an objective evil for the person. What is crucially at stake here, and is dialectically supportive of the self-evidency of the basic good of human life, is that death is a radical interference with the current life process of the kind of being that we are. In consequence, death itself can be credibly thought of as a ‘primitive evil’ for all persons, regardless of the extent to which they are currently or prospectively capable of participating in a full array of the goods of life.81 In conclusion, concerning willed human actions, it is justifiable to state that any intentional rejection of human life itself cannot therefore be warranted since it is an expression of an ultimate disvalue for the subject, namely, the destruction of the present person; a radical ontological good that we cannot begin to weigh objectively against the travails of life in a rational manner. To deal with the sources of disvalue (pain, suffering, etc.) we should not seek to irrationally destroy the person, the very source and condition of all human possibility.82

#### Court circumvention---they ignore intent and plain meaning, reject literature bias towards optimism.

Crane ‘21 [Daniel A Crane. Frederick Paul Furth, Sr. Professor of Law, University of Michigan. I am very grateful for many helpful comments from Tom Arthur, Jonathan Baker, Steve Calkins, Dale Collins, Eleanor Fox, Rebecca Haw, Hiba Hafiz, Jack Kirkwood, Bob Lande, Christopher Leslie, Alan Meese, Steve Ross, Danny Sokol, and other participants at the University of Florida Summer Antitrust Workshop. "ANTITRUST ANTITEXTUALISM." https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=4952&context=ndlr]

This view is so widely entrenched in the legal profession’s understanding of the antitrust laws—including, it must be admitted, this author’s—that it seems presumptuous to claim that the conventional wisdom is wrong, or at least significantly overstated. But it is. While the antitrust statutes may be lacking in some important particulars, they present a readily discernable meaning on many others. As Daniel Farber and Brett McDonnell have argued, “For the conscientious textualist, the statutory texts [of the antitrust laws] have considerably more specific meaning than the conventional wisdom would suggest.”5 And it is not simply the case that the meaning of the statutory texts could be rendered through ordinary methods of statutory interpretation but the courts have failed to see it. Rather, the courts frequently acknowledge that the statutory texts have a plain meaning, and then refuse to follow it.

But it gets worse. The courts have not merely abandoned statutory textualism or other modes of faithful interpretation out of a commitment to a dynamic common-law process. Rather, they have departed from text and original meaning in one consistent direction—toward reading down the antitrust statutes in favor of big business. As detailed in this Article, this unilateral process began almost immediately upon the promulgation of the Sherman Act and continues to this day. In brief: within their first decade of antitrust jurisprudence, the courts read an atextual rule of reason into section 1 of the Sherman Act to transform an absolute prohibition on agreements restraining trade into a flexible standard often invoked to bless large business combinations; after Congress passed two reform statutes in 1914, the courts incrementally read much of the textual distinctiveness out of the statutes to lessen their anticorporate bite; the courts have read the 1936 Robinson-Patman Act almost out of existence; and the Celler-Kefauver Amendments of 1950, faithfully followed in the years immediately after their promulgation, have been watered down to textually unrecognizable levels by judicial interpretation and agency practice. It is no exaggeration to say that not one of the principal substantive antitrust statutes has been consistently interpreted by the courts in a way faithful to its text or legislative intent, and that the arc of antitrust antitexualism has bent always in favor of capital.

#### Clarifying the scope and meaning of vague language doesn’t solve---courts ignore, Congress backs down, it’s already very clear.

Crane ‘21 [Daniel A Crane. Frederick Paul Furth, Sr. Professor of Law, University of Michigan. I am very grateful for many helpful comments from Tom Arthur, Jonathan Baker, Steve Calkins, Dale Collins, Eleanor Fox, Rebecca Haw, Hiba Hafiz, Jack Kirkwood, Bob Lande, Christopher Leslie, Alan Meese, Steve Ross, Danny Sokol, and other participants at the University of Florida Summer Antitrust Workshop. "ANTITRUST ANTITEXTUALISM." https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=4952&context=ndlr]

This Article has shown that, historically, the judiciary has treated the antitrust statutes as broad delegations to the courts to create a pragmatic common law of competition, even when the statutes plainly said something more specifically prohibitory. What, then, are the strategies available to a reformist Congress seeking to rein in business power through remedial antitrust legislation?

The one strategy that does not seem especially promising is simply writing clearer statutes. The antitrust statutes that the courts wrote down in favor of big business did not suffer from a lack of clarity or, if they did, not in the textual implications the courts chose to ignore. Strikingly, the courts continue to insist that the antitrust statutes are indeterminate delegations of common-law power, even while admitting in candor that they have simply chosen to ignore the statutes’ plain meaning in favor of a common method of deciding antitrust cases. For instance, in Professional Engineers, Justice Stevens remarked for the Court that “the language of § 1 of the Sherman Act . . . cannot mean what it says” and therefore that Congress must not have intended “the text of the Sherman Act to delineate the full meaning of the statute or its application in concrete situations,” thus justifying the courts in shaping the “statute’s broad mandate by drawing on common-law tradition.”255 Given over a century’s tradition of interpreting antitrust statutes as invitations to continue a common-law process whatever else is suggested by the statute’s text, it is difficult to see how simply accumulating stern new language in new texts would lead to a different result.

Even where reform statutes are textually honored in their immediate aftermath, history shows a creeping judicial tendency to begin integrating the reform statutes into the mainstream of antitrust jurisprudence within a few decades. This has been the fate of the four major antitrust reform statutes— the FTC, Clayton, Robinson-Patman, and Celler-Kefauver Acts—each of which was meant to rein in capital in ways that the Sherman Act did not. In all four instances, however, the courts incrementally began mainstreaming the statutes into Sherman Act precedent, creating a homogenous antitrust jurisprudence that read the textual distinctiveness out of the reform statutes. Thus, today, cases under the FTC Act, section 3 of the Clayton Act, and the Robinson-Patman Act are largely indistinct from Sherman Act cases,256 and merger cases have been rolled into the same modes of price-theoretic analysis that would be employed in a Sherman Act case.257 Given that neither statutory text nor legislative history seems to have deterred the courts from this process within a few decades after the passage of the statutes, there is little reason to believe that a “this time we mean it” statutory reform would not meet the same fate. If the courts continue to understand aspects of the antitrust statutes as aspirationally motivated and operationally impracticable, the previously observed pattern is likely to continue.