# Minnesota 1AC

### Innovation Advantage

#### Disparagement dooms biosimilar innovation---antitrust is key.

Carrier 2020, Michael A. Carrier Rutgers Law School Distinguished Professor (Northwestern Law Review 2020 “DON’T DIE! HOW BIOSIMILAR DISPARAGEMENT VIOLATES ANTITRUST LAW” https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3595785)//ellie

In the small-molecule setting, disparagement is not a concern. Brands are not likely to falsely injure near-identical generics, which garner sales not from advertising campaigns but from state laws that allow—and in many cases require—pharmacists to substitute generic versions of brand-name prescriptions.39 In contrast, the education of stakeholders is critical to the marketing of biologics and biosimilars,40 which has tempted biologic firms to engage in disparagement. There are four related categories of statements and omissions that biologic firms have made against biosimilars, none of which is consistent with the statute. The first category is the most dramatic. A January 2019 Washington Post article quotes Philip Schneider, chairman of the Alliance for Safe Biologic Medicines’ international advisory board, as suggesting caution in a move to unbranded biologics “so we don’t end up with another thalidomide [which famously caused birth defects]” or “all the other things that happen when safety isn’t considered.”41 Offering another example in the fearmongering category, the article further quotes a patient advocate affiliated with the group, who stated that a switch from one drug to another “disrupts your continuity of care,” as “[y]ou could end up in an emergency room, or be[] hospitalized, or try[] other, less efficient treatments,” all of which “can exacerbate or flare your disease, bring[ing] it out of remission.”42 The second group of assertions claims that the biosimilar acts differently from the reference product. In an Amgen YouTube video quoted in Pfizer’s citizen petition raising awareness of this issue, the company states that the two products “can behave differently in the body.”43 Amgen also tweeted: “Biologics or biosimilars? It’s not just apples to apples. While #biosimilars may be highly similar to their #biologic reference products, there’s still a chance that patients may react differently.”44 Janssen Biotech provides a similar, albeit more subtle, example. In a patient brochure, the company states that a patient “may be asked to switch to a biosimilar that works in a similar way to REMICADE,” but that “you and your doctor did a lot of fine tuning to get where you are now,” so “if your REMICADE® treatment is still working for you, talk to your doctor about staying on it.”45 The third category is based on claims that the biosimilar is not identical to the reference product. The Amgen video mentioned above states that “no two biologic medicines are identical.”46 Similarly, Genentech’s website, again as discussed in the Pfizer citizen petition, states that “FDA requires a biosimilar to be highly similar, but not identical” to the reference product.47 The fourth group emphasizes that biosimilars do not satisfy the standard of interchangeability. In the brochure mentioned above, Janssen states that “[e]ven though infliximab biosimilars are very similar to REMICADE®, that doesn’t mean they are interchangeable with REMICADE®.” Janssen also warned (in bolded statements) that “no infliximab biosimilar has been proven to be interchangeable with REMICADE®” and that “[t]he infliximab biosimilars are not approved as interchangeable with REMICADE®.”48 Each of these four categories can constitute disparagement. The first— consisting of threatening comparisons to Thalidomide and warnings of trips to the emergency room—needs no explanation. But each of the other categories also runs afoul of the statute’s requirements. The second category—that the biosimilar acts differently—fails to mention that the FDA only approves a biosimilar when it is “highly similar” to and has “no clinically meaningful differences” from the biologic product.49 In other words, the biologic and biosimilar products are required to have the same safety and effectiveness profile.50 As the FDA explained in Draft Guidance issued in February 2020, “representations or suggestions that create an impression that a biosimilar is not highly similar to its reference product are likely to be false or misleading.”51 Evidence from Europe, which has witnessed robust biosimilar market entry, has confirmed that more than “700 million patient days of treatment” demonstrated that “clinical outcomes with biosimilars match the outcomes of the reference biologics.”52 This evidence also has revealed that “patient[s] switching from the reference biologic to the biosimilar . . . is not of concern” since more than 14,000 switches resulted in “[n]o change in clinical outcomes.”53 As discussed below,54 disparaging statements, even if not completely false, are, at a minimum, deceptive in conveying the misleading interpretation that biosimilars have “clinically meaningful differences” from their reference biologics.55 The third category—claiming that the biosimilar is not identical— focuses on an issue that is irrelevant; in fact, it is “normal and expected within the manufacturing process” for even batches of biologic products themselves to reveal “[s]light differences.”56 In the Draft Guidance mentioned above, the FDA “remind[ed] firms that a biosimilar product is not required to be identical to the reference product” but that it need only be “highly similar to the reference product notwithstanding minor differences in clinically inactive components and that there are no clinically meaningful differences . . . in terms of safety, purity, and potency.”57 Finally, for the fourth category, a biosimilar’s failure to attain interchangeability does not mean that it is less safe. For starters, this status only makes sense for biosimilars that will be dispensed at the pharmacy counter (where substitution takes place), but each of the 15 biosimilars that has entered the U.S. market is dispensed in a hospital or infusion center.58 More fundamentally, as Pfizer pointed out in its citizen petition, its biosimilar “demonstrated that a single switch does not result in different safety or efficacy.”59 As the statement from the global regulatory authorities explained, “[a] full clinical development program[] is not necessary when extensive laboratory testing has demonstrated that the biosimilar is highly similar to the originator.”60 And as Boehringer Ingelheim explained in supporting Pfizer’s petition, “an FDA interchangeability designation is irrelevant” for “the majority of biologics . . . administered to the patient by the physician who has written the prescription,” with “misinformation . . . generated” to “impl[y] that interchangeable biologics are ‘better biosimilars’ . . . rather than the same biosimilar on which additional data has been generated.”61 II. REGULATORY SETTING How should courts analyze the antitrust effects of biologic firms’ disparagement of biosimilars? This Part sets the stage for the antitrust analysis by discussing the importance of the regulatory regime, showing the regime’s ineffectiveness, and highlighting the significant barriers to entry facing biosimilars. By brief way of background, the antitrust framework that applies to a single firm acting unilaterally is monopolization. This offense requires a showing of monopoly power and exclusionary conduct.62 Monopoly power is “the power to control prices or exclude competition.”63 Biologic firms that disparage biosimilars are likely to satisfy this element because of their ability to charge and sustain supracompetitive prices in a market characterized by significant barriers to entry.64 In contrast to monopoly power, the caselaw on exclusionary conduct is less clear. Courts often distinguish between the “willful acquisition or maintenance of [monopoly] power” and “growth or development as a consequence of a superior product, business acumen, or historic accident.”65 Considering the regulatory regime can shed critical light on the issue of exclusionary conduct. A. Regulatory Regime As the Supreme Court explained in Verizon Communications v. Trinko, the starting point for antitrust analysis is the regulatory regime. The Court stated that antitrust analysis must take “careful account” of “the pervasive federal and state regulation characteristic of the industry” and “recognize and reflect the distinctive economic and legal setting of the regulated industry to which it applies.”66 The Court in Trinko considered not just the existence of a regulatory regime, but also its effectiveness. In Trinko, the regime was working: phone companies providing local service were required to “be on good behavior” and not to discriminate in providing access before entering the long-distance market.67 Firms that did not satisfy these conditions were subject to financial penalties, weekly reporting requirements, or the suspension or revocation of long-distance approval.68 In contrast, regulatory abuse has prevented the biologics regime from operating as intended. The combination of ineffective FDA regulation and high barriers to entry ensures a role for antitrust.69 B. Ineffective Regulation Biosimilar competition in the United States is far from robust. In Europe, 59 biosimilars have received approval.70 In the United States, 27 biosimilars have been approved (with more than half the approvals occurring since July 2018).71 In addition, U.S. biosimilars have offered savings of only 15% to 35% (typically on the lower end), far less than the more significant (often 70%) discounts in Europe.72 The weak U.S. biosimilar market is not the consequence of the FDA’s lack of effort. In its citizen petition, Pfizer pointed to “various initiatives” the agency had undertaken “aimed at encouraging and facilitating the development and approval of biosimilars.”73 Such activities included “the numerous biosimilar-related guidance documents FDA has issued, the Agency’s development and distribution of educational materials . . . , the Agency’s Biosimilar User Fee Act performance goals, and the . . . Biosimilars Action Plan.”74 Despite these efforts, FDA officials have expressed frustration with the lack of biosimilar competition. In 2018, Former Commissioner Scott Gottlieb “worried” that the market for biosimilars “still isn’t established” and that “[t]he ability for these products to penetrate clinical practice, and gain acceptance, is still not firm.”75 In addition, Gottlieb lamented that biosimilar competition is “anemic” and that “the real savings” from biosimilars have been “just a fraction of even the most conservative initial estimates.”76 In fact, the agency found that “if Americans had the opportunity to purchase successfully marketed, FDA-approved biosimilar prescription drugs, they could have saved more than $4.5 billion in 2017.”77 Such savings, however, will not come to fruition if biologic companies “unfairly delay or derail the entry of biosimilar competitors” through conduct (discussed in the next Part) such as patent thickets and anticompetitive contracts.78 Gottlieb expressed further concern “that the biosimilar manufacturers may pull out” if biologics “are able to lock up markets even in cases where there’s a fully interchangeable competitor.”79 Even more on point, Gottlieb “worried” that “there are either deliberate or unintentional efforts by branded companies to create confusion” about biosimilars’ safety and effectiveness.80 These messages “can potentially undermine consumer confidence in biosimilars in ways that are untrue” and “negatively impact a patient’s judgment about an otherwise safe and effective product.”81 The FDA and FTC reiterated these concerns in a joint statement in February 2020 in which they explained that they “support competitive markets for biologics” and “have serious concerns about false or misleading statements and their negative impacts on public health and competition.”82

#### False advertisement wrecks biosimilars---maintaining competition with antitrust is key.

Carrier and Tushnet 21, Michael A. Carrier Rutgers Law School Distinguished Professor, Rebecca Tushnet Harvard Law School Professor of Law (Iowa Law Review 2021 “An Antitrust Framework for False Advertising” https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3593914)//ellie

An example illustrates our framework. The pharmaceutical industry is marked by high barriers to entry. It is expensive to enter the market, and there are significant hurdles such as receiving approval from the FDA. These barriers are even higher in the biologics setting. Compared to the “small molecule” drugs that have made up the pharmaceutical market for the past several decades, biologic products are more complex and less predictable. As a result, unlike the near-identical relationship between brand and generic drugs, the connection between biologics and “follow-on biosimilars” is not as direct.171 The relevant statute, the Biologics Price Competition and Innovation Act (“BPCIA”),172 requires a biosimilar to be “highly similar to” the biologic and have “no clinically meaningful differences” in relation to “safety, purity, and potency.”173 But the uncertainty surrounding the products has resulted in biologic manufacturers stating or implying that biosimilars are unsafe, sometimes by omitting relevant information about their functional equivalence with the reference biologics.174 In a setting in which even the most minute differences between products could be enough to dissuade patients from trying new medications, the assertions at least implied dissimilarities that could have significant safety effects. For example, Genentech noted on its “Examine Biosimilars” website that “FDA requires a biosimilar to be highly similar, but not identical to the [reference product].”175 More explicitly, Amgen tweeted: “Biologics or biosimilars? It’s not just apples to apples. While #biosimilars may be highly similar to their #biologic reference products, there’s still a chance that patients may react differently.”176 Given the context of life-saving medications, it’s easy to imply dire consequences. For example, Amgen created a YouTube video asserting that a switch “carries risks, given that no two biologic medicines are identical,” which suggests that they “can behave differently in the body.”177 Amgen also cautioned that “[s]witching drugs is not a good idea if your medicine is working for you” and that “an inadvertent substitution . . . is not appropriate care.”178 Finally, some biologic manufacturers have warned that patients could face “additional risks” by taking biosimilars or even “could end up in the emergency room.”179 These claims raise several concerns. Most significant, the statements at issue imply that biosimilars create serious risks, failing to disclose that the FDA approves a biosimilar only when “there are no clinically meaningful differences [from] the biologic product.”180 To the contrary, biologic and biosimilar products are required to have the same safety and effectiveness profile.181 Evidence from Europe, which has witnessed robust biosimilar entry, has confirmed that “over 700 million patient days of treatment” demonstrated “that clinical outcomes with biosimilars match the outcomes of the reference biologics.”182 This evidence also has revealed that “patient switching from the reference biologic to the biosimilar . . . is not of concern” since the more than 14,000 switches from biologic to biosimilar resulted in “[n]o change in clinical outcomes.”183 Given significant development costs, regulatory barriers, thickets of dozens of (or even more than 100) patents,184 and exclusive contractual arrangements,185 biologic manufacturers are likely to have monopoly power.186 Taking the absence of clinically meaningful differences in FDAapproved biosimilars as a given, plaintiffs challenging false statements are likely to satisfy our presumption if they can show that, under false advertising law, the statements (or omissions) are false and material, and therefore are likely to deceive consumers and cause harm. False advertising principles establish that biologic manufacturers will not be liable unless their statements are false or mislead substantial numbers of relevant consumers. But, if falsity or misleadingness are established, they are not likely to be able to rebut the presumption of anticompetitive conduct given the significance of health risk claims to consumers. Even for attempted monopolists, as long as a plaintiff establishes falsity or misleadingness, the factors would seem to favor liability. Given the lack of biosimilar entry to date, in many cases biosimilars will be seeking to enter the market. The statements, which focus directly on risk, pose significant barriers to entry, as doctors and consumers are not likely to take a chance on drugs that have even the possibility of safety concerns. It is hard to think of examples that would more concretely affect consumers than warnings that drug products are potentially unsafe. In fact, the FTC recently issued warning letters to a number of plaintiff-side law firms for advertising that linked FDA-approved drugs with serious side effects, potentially frightening patients away from useful medications.187 In addition, a biologic manufacturer’s disparagement of a biosimilar rival may be part of a broader range of anticompetitive conduct. For example, disparagement could entrench barriers to entry that convince insurance companies to favor biologics through potentially anticompetitive exclusive dealing, bundling, and rebates.188 In short, false advertising law provides useful tools for determining if substantial numbers of relevant consumers are being misled to their detriment. And our framework would likely find that a biologic manufacturer’s proven false advertising that raises safety concerns against a biosimilar constitutes monopolization.

#### Antitrust and biosimilar competition is make or break for the future of pharma

Marmaro, 21 – Morgan, Editor-in-Chief, Colum. J.L. & Soc. Probs., 2020-2021. J.D. Candidate 2021, Columbia Law School. Molecule Size Doesn't Matter: The Case for Harmonizing Antitrust Treatment of Pay-for-Delay Agreements, 54 Colum. J.L. & Soc. Probs. 169, Winter, p. Nexis – Iowa

In contrast, the FDA only recently developed the regulations allowing it to determine that a biosimilar is "interchangeable" with a biologic. 30 As of September 2020, the FDA has yet to designate a single biosimilar or biologic drug in the U.S as "interchangeable." 31 Indeed, the FDA has been relatively slow to even approve biologic and biosimilar drugs for sale in the U.S., making biosimilar introduction relatively slow in the U.S compared to Europe. 32 While there are seventy-one biosimilar drugs approved in Europe as of January 2020, only twenty-six biosimilars had been approved in the U.S. 33 But even when the FDA actually approves a biosimilar as an "interchangeable" drug, most states do not have laws that permit or mandate the substitution of the "interchangeable" drug with the biologic. 34 The pharmaceutical industry successfully lobbied for laws requiring naming conventions for biosimilar drugs that make it difficult for pharmacists to identify similar biologic drugs. 35 [\*177] States, for their part, have generally not updated their laws to provide more substitution of biosimilars or those drugs with interchangeability designations. However, with the end of the "golden age" for small-molecule brand drugs in sight and $200 billion in brand sales subject to generic competition by 2025, companies increasingly see biologics and biosimilars as the future of the pharmaceutical market. 36 As explained infra, biologic drugs' large price tag derives, in part, from a lack of meaningful competition in the U.S. and few pricing constraints. 37 Some $67 billion of the biologic market is vulnerable to biosimilar competition as major patents are set to expire in 2020; 38 the use of patents and pay-for-delay agreements by biologics companies remains a potent threat to any real competition. A class action, In re Humira (Adalimumab) Antitrust Litigation, 46alleges that AbbVie's multiple agreements are actually market allocating agreements and settlements qualifying as reverse payments. As of this writing, the In re Humira litigation is undergoing appeal after a district court ruled in favor of AbbVie, noting that while the behaviors seem unsavory, they were legal "exploited [\*179] advantages" derived from the current regulatory system. 47The court went further astray, finding that the agreements were not anticompetitive, and in contradiction with Actavis's rejection of the scope of the patent doctrine, did so by relying upon the alleged strength of AbbVie's Humira patents. 48But neither the parties nor the Court in In re Humira questioned the basic application of Actavis to the agreements in this case. Though the In re Humira district court dismissed the case in favor of defendants, 49this Note argues that the In re Humira district court was correct to engage in an Actavis analysis but did so incorrectly. A constrictive reading of Actavis to not include biologics, despite similar economic incentives to game the system and collusively divide the markets, would undoubtedly result in the proliferation of collusive biologic settlement agreements that will increase the already staggering biologic prices. There is clear congressional intent that supports treating biologic and small molecule collusive agreements under the same standards. 50 Further, using the ongoing In re Humira litigation as a framing device, an opportunity for courts to explicitly determine whether and how to apply the Actavis framework to biologic drug settlements, this Note will demonstrate how the reasoning and analysis of Actavis applies to qualifying settlements in the biologic sphere and is consistent with precedent, congressional intent, and public policy. While differences between biologics and small molecule pharmaceutical production warrant different FDA manufacturing [\*180] procedures, 51recent and ongoing legislative proposals addressing pay-for-delay agreements apply the same legal standards to adjudication of agreements for biologic and small molecule drug manufacturers. 52Some commentators, however, have advocated a narrow interpretation of Actavis to apply only to small molecule drugs 53because the Court only discusses the relevant regulatory framework for small molecule drugs in that case. 54They argue that the Actavis result was founded and based on the language and intent of the Hatch-Waxman Act. 55Just as the courts then spent years litigating whether Actavis only implicated cash-only "payments," 56savvy pharmaceutical attorneys are likely to argue that Actavis should apply only to drugs covered by the Hatch-Waxman Act. Part II will first discuss various forms of antitrust abuses that arise in the pharmaceutical space and are often utilized as part of or together with reverse payment agreements. It goes on to explain the legal and regulatory backgrounds of small and large molecule drugs, focusing on how the biologic regulatory regime differs. Part III then discusses the consequences of lax antitrust scrutiny on pharmaceuticals, and finishes with the allegations, arguments, and findings currently on appeal in In re Humira. Lastly, Part IV proposes a two-fold solution to the problems posed by Actavis's lack of legal clarity. First, there must be regulation or precedent that clearly indicates that for antitrust purposes, biologic settlement agreements should be subject to the same antitrust scrutiny as [\*181] those concerning small molecule drugs. In re Humira provides the perfect opportunity; and as the Part IV analysis will show, applying Actavis to biologics is in the spirit of the law, aligns with public policy, and follows precedent -- despite the In re Humira district court ruling in favor of the defendants. Second, this Note suggests a need for a corresponding legislative solution. This Note's purpose is to demonstrate that the way a drug is manufactured, approved, or allowed to compete does not alter the application of antitrust law seeking to rid the market of collusive agreements between rivals.

#### Pharma innovation solves disease, bioterror, and ABR.

Sonja Marjanovic and Carolina Feijao 20. \*Sonja Marjanovic; Director, Healthcare Innovation, Industry and Policy, RAND Europe. \*Carolina Feijao; Ph.D. in biochemistry, University of Cambridge; M.Sc. in quantitive biology, Imperial College London; B.Sc. in biology, University of Lisbon. “Pharmaceutical Innovation for Infectious Disease Management” RAND Corporation. 2020. https://www.rand.org/content/dam/rand/pubs/perspectives/PEA400/PEA407-1/RAND\_PEA407-1.pdf

As key actors in the healthcare innovation landscape, pharmaceutical and life sciences companies have been called on to develop medicines, vaccines and diagnostics for pressing public health challenges. The COVID-19 crisis is one such challenge, but there are many others. For example, MERS, SARS, Ebola, Zika and avian and swine flu are also infectious diseases that represent public health threats. Infectious agents such as anthrax, smallpox and tularemia could present threats in a bioterrorism context. The general threat to public health that is posed by antimicrobial resistance is also well-recognised as an area in need of pharmaceutical innovation. Innovating in response to these challenges does not always align well with pharmaceutical industry commercial models, shareholder expectations and competition within the industry. However, the expertise, networks and infrastructure that industry has within its reach, as well as public expectations and the moral imperative, make pharmaceutical companies and the wider life sciences sector an indispensable partner in the search for solutions that save lives. This perspective argues for the need to establish more sustainable and scalable ways of incentivising pharmaceutical innovation in response to infectious disease threats to public health. It considers both past and current examples of efforts to mobilise pharmaceutical innovation in high commercial risk areas, including in the context of current efforts to respond to the COVID-19 pandemic. In global pandemic crises like COVID-19, the urgency and scale of the crisis – as well as the spotlight placed on pharmaceutical companies – mean that contributing to the search for effective medicines, vaccines or diagnostics is essential for socially responsible companies in the sector. It is therefore unsurprising that we are seeing industry-wide efforts unfold at unprecedented scale and pace. Whereas there is always scope for more activity, industry is currently contributing in a variety of ways. Examples include pharmaceutical companies donating existing compounds to assess their utility in the fight against COVID19; screening existing compound libraries in-house or with partners to see if they can be repurposed; accelerating trials for potentially effective medicine or vaccine candidates; and in some cases rapidly accelerating in-house research and development to discover new treatments or vaccine agents and develop diagnostics tests. Pharmaceutical companies are collaborating with each other in some of these efforts and participating in global R&D partnerships (such as the Innovative Medicines Initiative effort to accelerate the development of potential therapies for COVID-19) and supporting national efforts to expand diagnosis and testing capacity and ensure affordable and ready access to potential solutions. The primary purpose of such innovation is to benefit patients and wider population health. Although there are also reputational benefits from involvement that can be realised across the industry, there are likely to be relatively few companies that are ‘commercial’ winners. Those who might gain substantial revenues will be under pressure not to be seen as profiting from the pandemic. In the United Kingdom for example, GSK has stated that it does not expect to profit from its COVID-19 related activities and that any gains will be invested in supporting research and long-term pandemic preparedness, as well as in developing products that would be affordable in the world’s poorest countries. Similarly, in the United States AbbVie has waived intellectual property rights for an existing combination product that is being tested for therapeutic potential against COVID-19, which would support affordability and allow for a supply of generics. Johnson & Johnson has stated that its potential vaccine – which is expected to begin trials – will be available on a not-for-profit basis during the pandemic. Pharma is mobilising substantial efforts to rise to the COVID-19 challenge at hand. However, we need to consider how pharmaceutical innovation for responding to emerging infectious diseases can best be enabled beyond the current crisis. Many public health threats (including those associated with other infectious diseases, bioterrorism agents and antimicrobial resistance) are urgently in need of pharmaceutical innovation, even if their impacts are not as visible to society as COVID-19 is in the immediate term. The pharmaceutical industry has responded to previous public health emergencies associated with infectious disease in recent times – for example those associated with Ebola and Zika outbreaks. However, it has done so to a lesser scale than for COVID-19 and with contributions from fewer companies. Similarly, levels of activity in response to the threat of antimicrobial resistance are still low. There are important policy questions as to whether – and how – industry could engage with such public health threats to an even greater extent under improved innovation conditions.

#### Disease causes extinction---the risk is categorically underestimated.

Dennis Pamlin & Stuart Armstrong 15. \*Executive Project Manager Global Risks, Global Challenges Foundation. \*\*James Martin Research Fellow, Future of Humanity Institute, Oxford Martin School, University of Oxford. February 2015, “Global Challenges: 12 Risks that threaten human civilization: The case for a new risk category,” Global Challenges Foundation, p.30-93. https://api.globalchallenges.org/static/wp-content/uploads/12-Risks-with-infinite-impact.pdf

A pandemic (from Greek πᾶν, pan, “all”, and δῆμος demos, “people”) is an epidemic of infectious disease that has spread through human populations across a large region; for instance several continents, or even worldwide. Here only worldwide events are included. A widespread endemic disease that is stable in terms of how many people become sick from it is not a pandemic. 260 84 Global Challenges – Twelve risks that threaten human civilisation – The case for a new category of risks 3.1 Current risks 3.1.4.1 Expected impact disaggregation 3.1.4.2 Probability Influenza subtypes266 Infectious diseases have been one of the greatest causes of mortality in history. Unlike many other global challenges pandemics have happened recently, as we can see where reasonably good data exist. Plotting historic epidemic fatalities on a log scale reveals that these tend to follow a power law with a small exponent: many plagues have been found to follow a power law with exponent 0.26.261 These kinds of power laws are heavy-tailed262 to a significant degree.263 In consequence most of the fatalities are accounted for by the top few events.264 If this law holds for future pandemics as well,265 then the majority of people who will die from epidemics will likely die from the single largest pandemic. Most epidemic fatalities follow a power law, with some extreme events – such as the Black Death and Spanish Flu – being even more deadly.267 There are other grounds for suspecting that such a highimpact epidemic will have a greater probability than usually assumed. All the features of an extremely devastating disease already exist in nature: essentially incurable (Ebola268), nearly always fatal (rabies269), extremely infectious (common cold270), and long incubation periods (HIV271). If a pathogen were to emerge that somehow combined these features (and influenza has demonstrated antigenic shift, the ability to combine features from different viruses272), its death toll would be extreme. Many relevant features of the world have changed considerably, making past comparisons problematic. The modern world has better sanitation and medical research, as well as national and supra-national institutions dedicated to combating diseases. Private insurers are also interested in modelling pandemic risks.273 Set against this is the fact that modern transport and dense human population allow infections to spread much more rapidly274, and there is the potential for urban slums to serve as breeding grounds for disease.275 Unlike events such as nuclear wars, pandemics would not damage the world’s infrastructure, and initial survivors would likely be resistant to the infection. And there would probably be survivors, if only in isolated locations. Hence the risk of a civilisation collapse would come from the ripple effect of the fatalities and the policy responses. These would include political and agricultural disruption as well as economic dislocation and damage to the world’s trade network (including the food trade). Extinction risk is only possible if the aftermath of the epidemic fragments and diminishes human society to the extent that recovery becomes impossible277 before humanity succumbs to other risks (such as climate change or further pandemics). Five important factors in estimating the probabilities and impacts of the challenge: 1. What the true probability distribution for pandemics is, especially at the tail. 2. The capacity of modern international health systems to deal with an extreme pandemic. 3. How fast medical research can proceed in an emergency. 4. How mobility of goods and people, as well as population density, will affect pandemic transmission. 5. Whether humans can develop novel and effective anti-pandemic solutions.

#### Affirmative prohibition is critical to innovation---creates a presumption of antitrust liability.

Carrier and Tushnet 21, Michael A. Carrier Rutgers Law School Distinguished Professor, Rebecca Tushnet Harvard Law School Professor of Law (Iowa Law Review 2021 “An Antitrust Framework for False Advertising” https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3593914)//ellie

One concern courts have raised with making false advertising the basis for an antitrust violation is that much of this behavior does not affect the market as a whole. Courts are right that even if one company engages in this conduct, and even if an individual rival is harmed as a result, that does not mean that competition in the market as a whole is affected. But there is a simple solution to this concern: focus on the defendant’s market power. Of all the actors employing false advertising, monopolists are the most likely to affect the market, with those attempting to monopolize making up the second-most-likely category. Targeting these two categories of actors recognizes that Section 2 of the Sherman Act provides the appropriate—and in fact only—framework for antitrust liability for unilateral conduct such as false advertising. Focusing attention on only monopolists and attempted monopolists dramatically narrows the universe of false advertising/antitrust claims. Such an emphasis also is consistent with the approach taken in the Areeda/Hovenkamp treatise, which recognizes that antitrust may be appropriate when “the practice makes a durable contribution to the defendant’s market power.”131 The treatise crafts a de minimis presumption because of the relative unlikelihood that any given false claim would “lead[] to or perpetuat[e] durable market power.”132 But the treatise also recognizes that “misrepresentations and organized deception by a dominant firm may have Section 2 implications when used against a nascent firm just as it is entering the market.”133 Once we understand that the treatise’s concerns about overapplication of false advertising law are addressed by requiring monopoly (or, as discussed below, attempted monopoly) status, the treatise would lend support to liability when the defendant’s monopoly power makes false advertising especially likely to affect the market as a whole and harm competition. Our focus on monopolists and attempted monopolists also is consistent with antitrust injury doctrine. As the Supreme Court famously explained in Brunswick Corp. v. Pueblo Bowl-O-Mat, Inc., plaintiffs must prove “injury of the type the antitrust laws were intended to prevent and that flows from that which makes defendants’ acts unlawful.”134 In other words, plaintiffs must challenge a harm that affects the market as a whole. Limiting our scrutiny to monopolists and attempted monopolists helps effectuate Brunswick’s objectives. We suggest a presumption that false advertising by monopolists constitutes monopolization. Crucially, the most fundamental critique against applying antitrust to false advertising—that “false advertising” does not require marketwide effects—are addressed by the defendant’s control over the market. To satisfy the first of the two elements of a monopolization case, a plaintiff must show that the defendant has monopoly power. As discussed above,135 a plaintiff can do so indirectly by showing a market share of at least 75 percent (and more likely 90 percent) along with barriers to entry that could entrench that market position. A plaintiff also can prove market power directly, such as by showing the defendant’s power to impose price increases or output reductions. Second, the plaintiff must show that the defendant engaged in false advertising. As a matter of underlying substantive law, liability for false advertising already requires findings that the defendant’s conduct was literally false or misleading, was material, actually deceived or was likely to deceive consumers, and caused or was likely to cause harm to the plaintiff.136 These elements are logically and practically linked to each other; they constitute the wrong of false advertising, just as an agreement to set prices constitutes the wrong of price fixing. In particular, deception is generally presumed from literal falsity, or is demonstrated by showing misleadingness—if consumers receive a false message from a facially ambiguous or even literally true claim, they have been deceived. Likewise, once both deception and materiality have been shown, courts generally find a likelihood of harm, as consumers have been misled about facts that are likely to affect their decisions. The false advertising foundation provides a unique advantage for antitrust law, one not available in other settings. The reason is simple. False advertising’s underlying requirements focus on the bad conduct, show its relevance, and demonstrate the harm. These elements offer on a silver platter what antitrust needs to prove monopolization. In addition, materially false advertising by a monopolist threatens multiple concerns: It makes it more difficult to compete on the merits, can easily be repurposed to harm any competitor, and is hard to credibly rebut without souring consumers on factual claims more generally. Because of these harms and the satisfaction of false advertising’s elements, a monopolist’s materially false advertising should be presumed to affect the market as a whole. A presumption that a monopolist using false advertising has engaged in illegal monopolization also is appropriate given the near certainty of anticompetitive effects. Unlike other lawbreaking by a monopolist such as tax fraud, false advertising by definition harms at least one competitor, in what is a relatively small field. That is, by definition a monopolist controls most of the market, so there will be fewer competitors to harm. False advertising may even directly harm all the other competitors if the false claim is one of general superiority, or, as in the AT&T example, is directed at keeping existing customers from switching products. And by poisoning the informational environment, false advertising inherently threatens the key mechanism by which rivals can compete: by explaining to consumers what they can offer in a way that might persuade them. False advertising is also a technique that can easily be extended to the next competitor, further justifying a presumption that its use by a monopolist caused harm to competition. Another way to frame the presumption of harm to competition centers on how we know that harm to actual entities has crossed into the legal category of “harm to competition.” When an entity that meets the standards for monopoly power engages in materially false advertising that causes damage, we know that it is a monopolist and that it harmed identified victims (such as consumers or competitors) in a way likely to push the market as a whole toward an untrusting and untrustworthy market for lemons. When a monopolist introduces a valuable innovation to the market, in contrast, that can harm competitors, but it also produces social benefit, meaning that the harm should be tolerated. So too when a monopolist truthfully and nonmisleadingly advertises a superior product. But when the ready-made template of false advertising law makes clear that a monopolist harms consumers’ ability to trust information in the market and causes consumers to pay prices or buy products they otherwise wouldn’t have chosen, at the very least the burden should be on the monopolist to show that it did no structural damage to the market.

#### American innovation solves global threat readiness---extinction from cyber, bio, chemical, and refugee-induced war.

Knipfer ’17 [Cody; Policy Associate at PoliSpace, M.A. Candidate in the Space Policy Institute at George Washington University; A Really Cool Blog, “On the Nature of Science and Technology Power,” <http://www.reallycoolblog.com/on-the-nature-of-science-and-technology-power/>]

Indeed, the United States’ leadership in science and technology has been a historical cornerstone of its capacity for “hard power” force application and projection and economic and societal “soft power.” It buttresses the country’s economic might, enables the modern standards of living of our citizenry, and expands our global cultural and normative reach.[ii] Equally so, the power of science and technology has been decisive in the context of national security. As President Truman noted in 1945, while urging Congress to create a Department of National Defense, “no aspect of military preparedness is more important than scientific research.” [iii] Through discoveries, technological innovation, and the capacity to develop ideas into deployable weapons, systems, and concepts, the United States has arrived at its modern-day military advantage and superiority.[iv]

To that end, science and technology may be considered key elements of the United States’ comprehensive national power – fundamentals of the country’s strength vis-à-vis competitors. Yet science and technology alone cannot ensure any country’s continued security, prosperity, or hegemony; far from operating in a vacuum, science and technology are constantly evolving to address changing domestic and international circumstances and threats. To reap advantage from science and technology, especially in their national security application, a country must continually innovate to tackle contemporary developments and anticipate future ones. This poses a considerable challenge, the solution to which extends beyond advanced engineering and research.

To explore these notions, this essay, particularly interested in the application of science and technology toward national security ends, examines the United States’ recent employment of security-related technologies. From this, it explores the attributes of science and technology power and the similarities and differences between science and technology power and other forms of national power such as the economic and diplomatic. Looking at the relative importance of science and technology in the United States today and likely significance in the coming future, it lays out a series of policy recommendations that may guide policymakers as they make decisions that impact the direction of the country’s scientific and technological course.

Employment of – and Challenges Facing – National Security-Related Technology

Recognizing the vital role that technology played in winning World War Two, along with the emerging threat of Soviet technological competitiveness, the United States established in the war’s wake an extensive infrastructure to support national security science and technology efforts. This provided foundation and catalyst for the development of military capabilities and tools needed to meet the challenges of the Cold War and the modern day: the nuclear triad, intelligence-gathering and cyber infrastructure, space-based radar and communications systems, advanced precision-guided munitions, and integrated command and control, along with myriad other assets.[v]

These technologies have seen extensive use in contemporary military conflicts. The wars in the Balkans and the Gulf saw the ever-increasing use of position, navigation, and timing assets such as GPS to provide precise and reliable information to the warfighter and direct precision-guided weaponry.[vi] Targeted airstrikes and weapons such as the long-range cruise missile have allowed for far more rapid, responsive, and accurate strikes than those of the past while substantially reducing collateral damage. Combat drones and unmanned aerial vehicles, innovations emblematic of the “War on Terror,” enable the warfighter to engage adversaries and conduct reconnaissance while safely remaining away from the front lines of the battlefield. Stealth aircraft, using a range of advanced technologies that reduce reflections and emissions, have helped pilots conduct sorties while evading detection.[vii]

Technology abets the United States’ security beyond warfighting. Advanced cyber capabilities – encryption, for example – seek to defend the networks which control the country’s power, transit, and water infrastructure from malicious hacks and crippling denial of service.[viii] Technologies capable of detecting harmful biological and chemical agents guard the country against potentially devastating attack by non-state actors.[ix] Increasingly sophisticated monitoring and surveillance technology enables the government to globally track and work to counter criminal activity, terrorist organizations, and other developments which threaten the country’s safety.[x]

Crucially, though, the United States’ contemporary application of national security systems has also demonstrated the inherent challenges of innovation and the limitations of technology. Despite advanced military hardware, principally designed to fight large-scale conventional wars against Cold War-era foes, the United States military had to “catch up” and react to unconventional tactics, such as roadside bombs and sniper attacks, employed against it in the Iraq and Afghanistan wars. Though decidedly outnumbered and outgunned, enemy combatants effectively countered the United States’ asymmetric technological advantage through guerilla warfare, propaganda, and exploiting collateral damage that advanced weapons systems created – doctrines which the United States’ technology did not anticipate and was unprepared or unsuited to counter.[xi] Likewise, despite the sophistication of the United States’ homeland security technologies, the government has struggled to prevent incidents of domestic terrorism such as mass shootings, often characterized by the use of simple, off-the-shelf equipment.[xii]

Meanwhile, in reaction to the United States’ present-day technological superiority, competitive foreign powers such as Russia and China are heavily investing in hardware and capabilities in the cyber and military realms specifically designed to counter the United States’ technological strengths and exploit its demonstrated vulnerabilities. The technological capabilities underlying the United States’ comparative military advantage are now proliferating to an increasing number of state and non-state actors, including potential adversaries, leveling the military “playing field.”[xiii]

The Attributes of National Security Science and Technology Power

From this, several key attributes and characteristics of science and technology as a form of national power can be identified. Foremost is the capacity for technology and science to be a significant, occasionally decisive, enhancer of a country’s military strength against enemies. Countries which develop innovative military technologies which effectively counter an adversary’s offenses or defensives, or against which an adversary has no means to protect itself, find themselves disproportionately advantaged on the battlefield. Indeed, technologies which upend dominant “status quo” warfighting paradigms – such as, historically, the introduction of the chariot, the tank, or nuclear weapons – are poised to significantly disrupt and reorder the geopolitical and military balance of power.[xiv]

To that end, science and technology power, particularly in the national security sphere, is developed and sustained through the adaption to, and more so through the anticipation of, revolutionary changes in military affairs, doctrine, and hardware. As Lieutenant Colonel Scott Stephenson noted in the influential “The Revolution in Military Affairs,” “those slow to adapt to military revolutions… are likely to suffer painful results. When the pace of change accelerates, the militaries that anticipate and adapt are likely to gain a massive advantage over potential enemies who are less agile.”[xv] That agility is, in large part, borne from innovations in science and the development of new technologies which lead to unanticipated, and therefore difficult to counter, doctrines.

A defining characteristic of science and technology power, then, is the continual quest for states to match, counter, and out-compete the technology of their adversaries. This continuing interplay between technology and national power, characterized by the sustained technological evolution and described often as an “offset,” has been a key focus for national security-related research and development throughout the Cold War and into the present. The United States’ deployment of nuclear weapons, for example, offset the numerical advantage held by the Soviet Union’s land forces in the early Cold War. Soviet parity in nuclear weapons catalyzed the development of guided weapon and integrated command and control as a counter, focusing on accuracy of targeted weapons systems independent of range.[xvi] The United States’ capacity to offset Soviet technology through innovative developments – and the Soviet bankruptcy borne from military expenditure that came as a corollary – was an important factor in maintaining a generally peaceful stable of power along with the country’s ultimate triumph in the Cold War. In the present-day, China and Russia’s focus on countering the systems and technologies which currently provide the United States’ military asymmetry is emblematic of this “offset” approach to science and technology power.

Paradoxically, however, national security-related technology in the present day has become as great an equalizer as it has historically been a separator of actors’ strengths. Technological superiority in the present may provide the United States’ unrivaled military strength, especially against foes (historically, state actors with large conventional forces) for which its national security technologies anticipated countering. Yet as the example of the Iraq and Afghani insurgencies amply demonstrated, technological superiority coupled with innovation focused on addressing hypothetical future battlefields may not be adequate to oppose or defeat all actors or all forms of warfare, regardless of the level of their sophistication.

Indeed, advanced technologies may be entirely vulnerable to actors utilizing doctrines with simple technologies that nonetheless exploit their weaknesses, as was the case with sophisticated – and expensive – American vehicles being destroyed by crude, homemade IEDs. Technology itself also creates weaknesses; the United States’ progressing economic and social reliance upon interconnected networks, for example, makes the country more vulnerable to potentially crippling attack. Despite advanced American cybersecurity technologies and techniques, non-state actors have still proven themselves capable of infiltrating, attacking, and even denying use of American cyber capabilities; considering recent trends, this vulnerable seems likely to continue, if not worsen.[xvii]

It may be that an attribute of science and technology power, borne more from the focus and perceptions of the technologists, theorists, and military leadership that employ it than from science and technology itself, is that it obscures other factors which equally dictate important developments in military, international, and geopolitical affairs. Political upheaval, social change, and economic development can change warfare dramatically, for example – and have nothing to do with “offset” strategies or war-room predictions of possible enemies’ future high-tech military hardware. As a product of the military-industrial complex that emerged in the Cold War United States to sustain continued technological development, Americans tend to be acutely – perhaps overly – sensitive to technological innovation among competitors and potential rivals. Fears during the Cold War and contemporary discussions of the “Third Offset” paint pictures of emerging, potential, and fanciful enemy weapon systems – which military planning and technology development was and is oriented toward countering.[xviii] This fixation on solutions entailing engineering and technological complexity blinds the national security technology apparatus to external trends that could definitively impact the future course of war – such as the collapse of the Soviet Union leaving the United States with a high-tech military and warfighting doctrine unsuited for the military pressures and asymmetric nature of counterinsurgency; the rise of radical terrorism with ideological underpinnings that condone unconventional guerilla tactics such as suicide bombings, which had great effect against high-tech targets; or the continuing crisis where lone-wolf gunmen using off-the-shelf rifles can commit massacres despite the government’s highly complex and pervasive surveillance and monitoring technology.

Similarities and Differences to Other Forms of National Power

With these attributes in mind, a comparison can be drawn between science and technology power and other forms of power which constitute a country’s comprehensive strength, such as the economic and diplomatic. Regarding the economic, science and technology power is similar in that the development of science and technology is driven by the same forces as economic growth. Like new economic products, services, and methods of operation, science and technology power relies upon the ingenuity of human actors predicting and anticipating future trends, possibilities, and human behavior. Innovation, iteration, and competitiveness are fundamental catalysts for the continued evolution and growth of both. The rapid proliferation and subsequent use of innovative technologies across the world quickly equalizes both the national security advantage and the economic advantage they provided their inventor.

Economic power, like national security technology, is a key element of a country’s warfighting capability – industrial might, strength in quality production, and capable infrastructure are crucial facets of a country’s ability to mobilize and project force. A fundamental difference between economic power and science and technology power, however, is competition. While economies naturally compete, there is incentive for states to specialize in the economic product or service most suited for it – their comparative advantage. Competing economies are not actively incentivized to counter the economic specialization of their rivals. With science and technology power for national security use, however, states decidedly hope to actively and explicitly counter the relative advantage of their adversaries.

Like diplomatic power, science and technology has a “soft power” element; other states and their societies may be influenced or compelled to action by the might, prestige, or cultural and technological hegemony of a country in possession of highly advanced and capable technologies.[xix] Diplomatic power occasionally experiences the same issue of science and technology policy in being blinded to unpredicted or external trends in the social, cultural, and economic spheres. The power of diplomacy, for example, did not anticipate and struggled to deal with the cultural, social, and political circumstances that led to a breakdown of order in post-invasion Iraq; just as national security technology was unprepared for the guerilla warfare of the Iraqi insurgency. Diplomatic power and science and technology power differ, though, in the fields of innovation and evolution. Whereas the military regime is constantly evolving and occasionally being upended by revolutions in security technology and associated doctrine, the Westphalian diplomatic order has remained largely similar through centuries – even as it has grown gradually more complex and interconnected. States do not tend seek to outcompete each other in the diplomatic sphere through revolutionary new approaches to diplomacy; negotiations, sanctions, deals, bi- and multilateral agreements, and the like have remained consistent “doctrines” employed by states in their dealings with international friends and foes.

Science and Technology Power’s Present and Future Importance

To return to Vannevar Bush’s assertion over half a century ago, science and technology is crucially important for a states’ economic growth and prosperity, the wellbeing of its citizens, and national security. This remains absolutely the case today. Despite the challenges facing innovation in the face of unanticipated adversaries and the proliferation of advanced, equalizing technologies among adversarial states and non-state actors, science and technology provides the United States’ unrivaled levels of security and military hegemony.

With the appearance of significant global challenges – refugee crises, environmental degradation, the possible emergence of a bi- or multi-polar world characterized by states with rough or equal technological parity, to name a few – the future importance of science and technology power cutting across all aspects of national security will undoubtedly redouble. Science and technology and its application as an element of the United States’ national power will need to be directed to address these challenges. While the exact characteristics that will define domestic and foreign national security technologies of the future – not to mention the economic and social – remain uncertain, the United States cannot afford to permit its current technological advantage to slip. Indeed, as revision states such as China continue to develop their technologies to directly counter the United States’ capabilities, it will likely become an imperative for the country to more actively engage in and support the development of innovative new security technologies and doctrines – lest, as history would suggest, the international order again be upended.

#### Alternative regulations fail and suppress competition.

Carrier and Tushnet 21, Michael A. Carrier Rutgers Law School Distinguished Professor, Rebecca Tushnet Harvard Law School Professor of Law (Iowa Law Review 2021 “An Antitrust Framework for False Advertising” https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3593914)//ellie

False advertising liability alone cannot address the marketwide harms caused by deceptive behavior. This Section first addresses antitrust’s comparative advantage for marketwide harms. It then offers examples of antitrust properly targeting conduct that violates other, non-antitrust laws, demonstrating that antitrust’s treatment of false advertising is an outlier. It concludes by showing that false advertising’s remedies cannot fully protect competition on their own. 1. Antitrust’s Comparative Advantage An antitrust-based framework for false advertising claims is necessary because of the unique role that the discipline can play. When companies engaging in false advertising have monopoly power, they possess the ability to harm not only an individual competitor but also the market as a whole. The consequences can be significant, especially for nascent competitors not able to enter the market, as the deception of consumers deprives them of the opportunity to obtain lower prices, more options, or enhanced quality. One way to understand the harms of false advertising to the market as a whole is revealed by George Akerlof’s classic explanation of the market for lemons.99 As Akerlof explains, in the absence of some way to guarantee the truth of claims about products, such as a used car’s quality, consumers reasonably respond by discounting all such claims. This distrust means that producers with actually superior products cannot charge the amount consumers would pay if they believed the superiority claim, which pushes superior (but more expensive to produce) products out of the market. If truthful advertisers are not able to guarantee their claims, producers unable to compete on their product characteristics suffer. And consumers are harmed by an unattractive (and perhaps even harmful, in the case of false health or safety claims) mix of products. Meanwhile, many false advertising techniques can be readily repurposed for new uses, meaning that a false advertiser can go from success to success in the absence of false advertising liability.100 Regulation that suppresses false claims—especially where such claims are most likely to have an effect—thus does more than protect individual consumers from fraud. It allows truthful producers to compete on a level playing field. In other words, addressing false advertising protects competition, not just competitors. The Supreme Court relied on Akerlof’s insights when it endorsed the pro-competitive effects of restrictions on false advertising. In California Dental Ass’n v. FTC, the Court addressed a dental association’s attempts to restrict “false or misleading” advertising that imposed significant limits on advertising “low prices” or other general price claims.101 The Court rejected the idea that such limits were inherently anticompetitive. Especially where information is hard to evaluate, even broad restrictions with the aim of preventing false advertising can be procompetitive.102 When false advertising threatens harms to the market as a whole, antitrust liability offers advantages over false advertising law. For starters, antitrust offers a more powerful toolkit deterring this conduct. Although false advertising law allows recovery of damages (albeit not as a penalty) and disgorgement of the profits from false advertising, courts impose high barriers to disgorgement, including requiring a showing of willfulness. In addition, courts have required plaintiffs to show a robust connection to the harm suffered to receive damages or disgorgement of profits. As a result, courts have denied awards in precisely the cases of concern: where there are a small number of potential competitors and where some of the monopolist’s gains from false advertising likely came at the expense of the overall market rather than a single plaintiff, making it difficult to allocate false advertising-based damage awards.103 There are two key ways in which antitrust offers more powerful protection against monopolists’ false advertising than federal false advertising law: remedies and eligible plaintiffs. First, antitrust offers the more powerful remedies of treble damages and automatic (as opposed to the Lanham Act’s exceptional104) attorneys’ fees that promise to provide robust deterrence against companies considering this behavior. Antitrust also offers injunctive relief preventing the continuation of the conduct. While a Lanham Act false advertising injunction generally is limited to the specific false claims that have been proven, an antitrust injunction could more generally target false advertising and marketwide harm to competition.105 Antitrust offers a more expansive territorial jurisdiction.106

### Plan

#### The United States federal government should substantially increase prohibitions on false advertising by applying a presumption that monopolists engaging in false advertising violate antitrust law and are subject to Penalty Offense Authority enforcement by the Federal Trade Commission.

### FTC Advantage

#### **FTC failure to prohibit false advertising is an existential threat to the agency. Market-wide Section 5 penalty offense authority (POA) restores FTC credibility, boosts fraud deterrence, and reduces litigation**

Lee, 21 – Bethany, J.D. Candidate, University of Pennsylvania Law School. “Reviving the Power of the FTC,” The Regulatory Review, May 17, <https://www.theregreview.org/2021/03/17/lee-reviving-power-of-ftc/> -- Iowa

The Federal Trade Commission (FTC) may face an existential threat to its ability to hold corporate lawbreakers accountable. A pending U.S. Supreme Court case threatens the FTC’s ability to seek monetary relief from wrongdoers, while mounting public concerns about the adequacy of the FTC’s enforcement have led to a crisis of confidence in the agency.

The solution to this urgent crisis involves restoring a key FTC authority, according to a new paper by FTC Commissioner Rohit Chopra and his attorney advisor Samuel Levine.

After tracing the history of the FTC’s enforcement tools and explaining their current inadequacy, Chopra and Levine argue that reviving the FTC’s Penalty Offense Authority will improve the FTC’s effectiveness and regain public confidence by increasing deterrence and ensuring fairness for honest firms.

Established by the FTC Act, the FTC has a mission to “protect consumers and competition by preventing anticompetitive, deceptive, and unfair business practices.” Chopra and Levine, however, highlight the FTC’s concerning track record in fulfilling this mission.

In the 1980s, the FTC’s leadership viewed markets as self-correcting, and the agency shifted its focus from market-wide abuses to “small-scale criminal fraud.” Seeking to avoid the derisive label of a “national nanny,” the FTC began to disarm the administrative state by halving the agency’s staff, reversing rulemakings, and adopting policies restricting the agency’s own authority.

The FTC’s ideology of the 1980s had lasting consequences, according to Chopra and Levine. In the 1990s, the agency failed to challenge tobacco advertising directed at children. In the 2000s, the FTC took minimal enforcement action to prevent the mortgage meltdown, remaining largely idle as subprime lenders sold loans structured to fail. Congress responded by stripping the FTC of major authorities over the financial sector, such as rulemaking on mortgages and debt collection.

Chopra and Levine argue that the agency’s inaction over several decades has resulted in “massive harm for consumers, small businesses, and the economy.” They call for a shift toward “systematic efforts to combat widespread harms.”

A key step, say Chopra and Levine, involves resurrecting the agency’s Penalty Offense Authority. Codified in Section 5 of the FTC Act, this provision allows the FTC to correct and deter harmful practices.

Currently, the FTC largely relies on Section 13(b) of the FTC Act, which allows the agency to seek preliminary and permanent relief in federal court. But the use of Section 13(b) has been challenged in multiple cases, including in a pending U.S. Supreme Court case challenging the FTC’s authority to seek equitable monetary relief.

Even if courts uphold the use of Section 13(b), argue Chopra and Levine, this enforcement tool remains inadequate in correcting and deterring widespread harms. To seek monetary relief under Section 13(b), the FTC must approximate harms or unjust gains—a potentially difficult and costly calculation. As a result, the FTC often resorts to no-money settlements that do not adequately deter wrongdoing. In addition, corporate wrongdoers tend to be undeterred by equitable relief sought under Section 13(b) since the worst consequence merely involves returning their earnings.

Instead of overreliance on Section 13(b), Chopra and Levine advocate greater use of the Penalty Offense Authority under Section 5 of the FTC Act. Under this authority, the FTC can seek civil penalties if the agency issued a final cease-and-desist order determining that a practice is unfair or deceptive and if a party subsequently engaged in that practice, knowing that the practice was unfair or deceptive.

Chopra and Levine note that the Penalty Offense Authority provides “strong due process protections for defendants.” For example, parties cannot be held liable unless shown to have actual knowledge of the FTC’s determination. Defendants can also challenge the FTC’s prior determination that the conduct was unlawful.

Previously, the FTC deployed its Penalty Offense Authority to target whole industries, in a manner that one FTC commissioner described as “extremely effective and efficient.” Nevertheless, the agency’s use of this tool rapidly declined in the 1980s, and it was used only once in the last decade.

Calling for renewed use of the Penalty Offense Authority, Chopra and Levine outline three key benefits of such a resurrection. First, compared to equitable relief, civil penalties would more effectively punish and deter wrongdoers. Second, the use of the Penalty Offense Authority would reduce litigation risk for the FTC. Current overreliance on Section 13(b) creates uncertainty as court cases challenge the program, and seeking monetary relief under Section 13(b) requires risky and expensive attempts to quantify harm. Finally, the Penalty Offense Authority provides market-wide impact. By providing notice to firms across an industry, the FTC can correct market-wide practices—increasing compliance and reducing the need to bring similar enforcement actions repeatedly.

Chopra and Levine specifically advocate the use of the Penalty Offense Authority in areas where a harmful practice has been condemned by an FTC order but not forbidden by an agency rule. They identify five areas where the FTC could deploy the Penalty Offense Authority based on existing orders: for-profit college fraud, false earnings claims targeted at workers, online disinformation, deceptive data harvesting, and illegal targeted marketing.

Ultimately, Chopra and Levine call on the FTC to shed its “self-inflicted paralysis” by drawing on a broader set of tools to protect the public.

#### Section 5 is the only avenue for fraud crackdowns

Olsen & Schultze 21, Christopher Olsen is a partner in the privacy and cybersecurity practice at Wilson Sonsini and Vice Chair of the Privacy and Information Security Committee of the ABA Antitrust Law Section, and former Deputy Director of the FTC’s Bureau of Consumer Protection; Stephen Schultze is an Associate in the privacy and cybersecurity practice at Wilson Sonsini, “FTC Authority Under Siege: Monetary and Injunctive Relief at Risk in Courts as Congress Contemplates a Response,” The Antitrust Source, April 2021, ABA

It is hard to imagine a favorable outcome for the FTC after this oral argument. The Court will probably limit 13(b) relief to injunctions, requiring the Commission to resort to cumbersome administrative proceedings to get any monetary relief. That would dramatically undermine the Commission’s work over several decades to build a robust fraud program.40 It would leave Section 5 and 19 as the only avenues for monetary relief under the FTC’s general consumer protection authority. Under Section 5, the Commission may impose monetary civil penalties under some limited circumstances.41 Under Section 19, the Commission may obtain monetary consumer redress or disgorgement but only after obtaining a final cease-and-desist order through administrative litigation and only after demonstrating that “a reasonable man would have known under the circumstances [that the conduct] was dishonest or fraudulent.”42 Moreover, Section 19 includes a statute of limitations whereas Section 13(b) does not.43 Thus, the FTC has strongly favored Section 13(b) actions. At oral argument, the FTC conceded that going directly to court is “more attractive in certain instances” and that the Commission brings “far more [consumer protection] cases” in court than through its own administrative proceedings.

#### Fraud crackdowns stop major terror attacks

Michael Tierney 18, George & Mary Hylton Professor of International Relations; Director Global Research Institute (GRI), “#TerroristFinancing: An Examination of Terrorism Financing via the Internet,” International Journal of Cyber Warfare and Terrorism, vol. 8, no. 1, 01/2018, pp. 1–11

2. TERRORIST FINANCING AND THE INTERNET

As mentioned, terrorists’ use of the internet has become a major concern for security officials across the world in recent years. Like many other users, terrorists have found that the internet is an invaluable tool to share information quickly, in order to disseminate ideas and link up with likeminded individuals (Jacobson, 2010; Okolie-Osemene & Okoh, 2015). In this manner, terrorists use the internet for a variety of purposes, including recruitment, propaganda, and financing. As scholars have also noted, the internet is an attractive option for extremists due to the security and anonymity it provides (Jacobson, 2010). Yet while there have been a growing number of studies completed on the ways in which terrorist organizations use the internet to recruit and indoctrinate others, there has been relatively little focus on the methods by which terrorists finance themselves through online activities. Some researchers have attempted to fill gaps in this area by broadly studying internet aspects of terrorism financing. However, research on this particular aspect of terrorism financing still appears to be lacking, with little focus on new methods of terrorist financing via the internet or a marrying of strategies to combat online financing trends available to practitioners in the field.

For instance, Sean Paul Ashley (2012) assessed the mobile banking phenomenon, which is prevalent in regions such as the Middle East and Africa, and provides extremists with the ability to easily connect to the internet and remit funds around the world. The decentralization of this kind of banking, due to the fact that brick-and-mortar facilities are not needed to conduct transactions, has allowed terrorist financiersto more efficiently move funds while avoiding detection from authorities. Other researchers,such as MichaelJacobson (2010), have studied the waysin which terrorists engage in cyber-crime to raise and move funds. For example, Jacobson (2010) found that online credit card fraud was a fairly major source of terrorist financing. By stealing a victim’s private credit information, terrorists are able to co-opt needed funds and provide support to themselves or their counterparts. Yet as James Okolie-Osemene and Rosemary Ifeanyi Okoh (2015) note, the internet is mostly used to augment and assist activities which occur in the physical world. In this way, it would appear that the internet is far more useful as a means to move funds globally in support of terrorism, rather than simply as a method to raise funds.

#### High risk of nuclear terror.

CACNP 21 – (The Center for Arms Control and Non-Proliferation is a national nonpartisan nonprofit dedicated to enhancing peace and security through expert policy analysis and thought-provoking research. “Fact Sheet: Nuclear Terrorism: A Clear and Present Danger.” <https://armscontrolcenter.org/nuclear-terrorism-a-clear-and-present-danger/>, Last Updated March 2021 //ROBBIE)

Nuclear terrorism – the threat by a terrorist group to obtain and use a nuclear weapon, or to acquire enough nuclear material to create and use a crude weapon or dirty bomb – poses a serious threat to the United States and its allies. A Pentagon review of U.S. nuclear policy indicated that nuclear terrorism is the “most immediate and extreme danger” facing the United States. With just 25 kilograms worth of highly enriched uranium (HEU), small enough to fit in a suitcase, terrorists could make a nuclear weapon capable of inflicting the same devastation as the bombs used at Hiroshima and Nagasaki. Terrorists could also lace conventional explosives with radiological material to create a dirty bomb. A dirty bomb, while not as lethal as a nuclear weapon, is considered a weapon of mass disruption due to the widespread panic associated with the weapon’s radiological fallout. According to a 2011 Congressional Research report, a dirty bomb detonation would have six major consequences: immediate casualties from conventional detonation, panic, economic disruption, long-term evacuations, exorbitant decontamination costs, and long-term casualties from cancer. What Can Be Done? To address these threats, the United States and Russia, the two countries with the largest stockpiles of nuclear material, have worked together to secure nuclear weapons and facilities. These programs have also been extended to other countries with nuclear facilities and materials that could be at risk. There has been considerable progress over the last several decades to reduce the probability that terrorists might acquire nuclear material. These efforts include the complete removal of civilian highly enriched uranium from 30 countries and Taiwan and the conversion or closure of at least 94 research reactors that formerly used highly enriched materials. But there is still significant work to be done. There remains nearly 2,000 metric tons of weapons-usable nuclear material spread across the globe, some of it vulnerable to theft or sabotage. There are abundant examples of lax security standards, including the break-in at the U.S. maximum security facility for nuclear materials led by an unarmed 82-year old nun, an armed break-in at a South African nuclear facility in 2007, and at least 167 incidents in 2019 in which nuclear or radiological material was lost, stolen, or outside of authorized control. Programs tasked with securing these materials hovered around $2 billion under the Trump administration, which takes the funding and attention back to pre-2013 levels. Congressional appropriations for core nuclear security programs declined in the end of the Obama administration’s second term after the success of a series of Nuclear Security Summits. However, according to Sen. Dianne Feinstein (D- Calif.), the funding reduction led to a five-year delay for securing and converting nuclear reactors across the globe, pushing the completion of that project to 2035. [Chart Omitted] To prevent a nuclear terrorism incident, the United States and its international partners must secure radiological and fissile material with the goal of maintaining the highest security standards. Nuclear non-proliferation programs should receive full funding and support from both Congress and the White House.

#### That causes nuclear war---cash is key

Dr. Peter J. Hayes 18, Executive Director of the Nautilus Institute for Security and Sustainability, Ph.D. in Energy and Resources from the University of California-Berkeley, Professor of International Relations at RMIT University, “Non-State Terrorism and Inadvertent Nuclear War”, NAPSNet Special Reports, 1/18/2018, <https://nautilus.org/napsnet/napsnet-special-reports/non-state-terrorism-and-inadvertent-nuclear-war/>

The critical issue is how a nuclear terrorist attack may “catalyze” inter-state nuclear war, especially the NC3 systems that inform and partly determine how leaders respond to nuclear threat. Current conditions in Northeast Asia suggest that multiple precursory conditions for nuclear terrorism already exist or exist in nascent form. In Japan, for example, low-level, individual, terroristic violence with nuclear materials, against nuclear facilities, is real. In all countries of the region, the risk of diversion of nuclear material is real, although the risk is likely higher due to volume and laxity of security in some countries of the region than in others. In all countries, the risk of an insider “sleeper” threat is real in security and nuclear agencies, and such insiders already operated in actual terrorist organizations. Insider corruption is also observable in nuclear fuel cycle agencies in all countries of the region. The threat of extortion to induce insider cooperation is also real in all countries. The possibility of a cult attempting to build and buy nuclear weapons is real and has already occurred in the region.[15] Cyber-terrorism against nuclear reactors is real and such attacks have already taken place in South Korea (although it remains difficult to attribute the source of the attacks with certainty). The stand-off ballistic and drone threat to nuclear weapons and fuel cycle facilities is real in the region, including from non-state actors, some of whom have already adopted and used such technology almost instantly from when it becomes accessible (for example, drones).[16]

Two other broad risk factors are also present in the region. The social and political conditions for extreme ethnic and xenophobic nationalism are emerging in China, Korea, Japan, and Russia. Although there has been no risk of attack on or loss of control over nuclear weapons since their removal from Japan in 1972 and from South Korea in 1991, this risk continues to exist in North Korea, China, and Russia, and to the extent that they are deployed on aircraft and ships of these and other nuclear weapons states (including submarines) deployed in the region’s high seas, also outside their territorial borders.

The most conducive circumstance for catalysis to occur due to a nuclear terrorist attack might involve the following nexi of timing and conditions:

1. Low-level, tactical, or random individual terrorist attacks for whatever reasons, even assassination of national leaders, up to and including dirty radiological bomb attacks, that overlap with inter-state crisis dynamics in ways that affect state decisions to threaten with or to use nuclear weapons. This might be undertaken by an opportunist nuclear terrorist entity in search of rapid and high political impact.
2. Attacks on major national or international events in each country to maximize terror and to de-legitimate national leaders and whole governments. In Japan, for example, more than ten heads of state and senior ministerial international meetings are held each year. For the strategic nuclear terrorist, patiently acquiring higher level nuclear threat capabilities for such attacks and then staging them to maximum effect could accrue strategic gains.
3. Attacks or threatened attacks, including deception and disguised attacks, will have maximum leverage when nuclear-armed states are near or on the brink of war or during a national crisis (such as Fukushima), when intelligence agencies, national leaders, facility operators, surveillance and policing agencies, and first responders are already maximally committed and over-extended.

At this point, we note an important caveat to the original concept of catalytic nuclear war as it might pertain to nuclear terrorist threats or attacks. Although an attack might be disguised so that it is attributed to a nuclear-armed state, or a ruse might be undertaken to threaten such attacks by deception, in reality a catalytic strike by a nuclear weapons state in conditions of mutual vulnerability to nuclear retaliation for such a strike from other nuclear armed states would be highly irrational.

Accordingly, the effect of nuclear terrorism involving a nuclear detonation or major radiological release may not of itself be *catalytic* of *nuclear* war—at least not intentionally–because it will not lead directly to the destruction of a targeted nuclear-armed state. Rather, it may be catalytic of non-nuclear war between states, especially if the non-state actor turns out to be aligned with or sponsored by a state (in many Japanese minds, the natural candidate for the perpetrator of such an attack is the pro-North Korean General Association of Korean Residents, often called Chosen Soren, which represents many of the otherwise stateless Koreans who were born and live in Japan) and a further sequence of coincident events is necessary to drive escalation to the point of nuclear first use by a state. Also, the catalyst—the non-state actor–is almost assured of discovery and destruction either during the attack itself (if it takes the form of a nuclear suicide attack then self-immolation is assured) or as a result of a search-and-destroy campaign from the targeted state (unless the targeted government is annihilated by the initial terrorist nuclear attack).

It follows that the effects of a non-state nuclear attack may be characterized better as a *trigger* effect, bringing about a *cascade* of nuclear use decisions within NC3 systems that shift each state increasingly away from nuclear non-use and increasingly towards nuclear use by releasing negative controls and enhancing positive controls in multiple action-reaction escalation spirals (depending on how many nuclear armed states are party to an inter-state conflict that is already underway at the time of the non-state nuclear attack); and/or by inducing concatenating nuclear attacks across geographically proximate nuclear weapons forces of states already caught in the crossfire of nuclear threat or attacks of their own making before a nuclear terrorist attack.[17]

#### **Massive attacks on critical infrastructure are underway – FTC deterrence credibility is make or break**

Pfefferkorn, 1-13-22 – Riana, research scholar at the Stanford Internet Observatory. “Why the FTC is telling companies to patch Log4j vulnerabilities,” Brookings Institute – Tech Stream, <https://www.brookings.edu/techstream/why-the-ftc-is-telling-companies-to-patch-log4j-vulnerabilities/> -- Iowa

For cybersecurity workers, 2021 ended with a bang. On Dec. 9, a severe zero-day vulnerability was publicly disclosed in Log4j, a widely used Java logging utility. Dubbed Log4Shell, the flaw allowed an attacker to remotely gain control of a vulnerable device that used the utility. Given Java’s ubiquity, this meant that hundreds of millions of devices were at risk, ranging from servers for enterprise software, cloud hosting, and web applications, to consumer devices such as smart TVs and internet-connected security cameras. What’s more, the flaw was easy to exploit, rendering it accessible to bad actors with no need for high levels of skill, sophistication, or resources. The head of the U.S. Cybersecurity and Infrastructure Security Agency (CISA), Jen Easterly, called the Log4j flaw one of the most serious vulnerabilities she’d ever seen.

As 2022 begins, the crisis shows no sign of abating. Remediation efforts continue, while attackers are probing systems looking for Log4j vulnerabilities. On Jan. 3, security experts at Microsoft wrote that they expect this issue “to have a long tail for remediation, requiring ongoing, sustainable vigilance.” The company has already observed state-backed hackers from China, Iran, and North Korea attempting to exploit the Log4j vulnerability, and Easterly foresees that attackers will keep doing so “well into the future.” The coming year is likely to see more attacks on critical infrastructure, more ransomware attacks against public and private networks—and increased risk to the security of Americans’ personal, financial, and other sensitive data. That’s because, like it or not, private-sector companies hold vast amounts of information about us, on systems whose security is beyond our control. Yet the United States doesn’t yet have a generally applicable federal law that would impose minimum data security requirements on the private sector. So how will our government defend Americans’ data security against the Log4j threat?

In the absence of broad data-security rules, several U.S. regulators are stepping up to address Log4j. CISA, for example, has mandated that the sprawling array of civilian federal computer networks be updated to address the Log4j vulnerability. The deadline to do so was Dec. 23, but the work is ongoing. The Federal Trade Commission, for its part, is engaging with the private sector by warning companies that they could be subject to legal action if they fail to remediate the Log4j vulnerability.

On Jan. 4, the FTC published a blog post reminding companies that they have a legal “duty to take reasonable steps to mitigate known software vulnerabilities.” It threatened to bring the full force of the agency’s authority against “companies that fail to take reasonable steps to protect consumer data from exposure as a result of Log4j, or similar known vulnerabilities in the future.” The warning cited the $700 million it cost Equifax to settle multiple enforcement actions stemming from a 2017 data breach that affected 147 million people due to the company’s failure to patch a known security vulnerability.

You might be wondering: why the FTC? And why Jan. 4, almost four weeks after Log4Shell’s public disclosure? CISA has been all over the Log4j vulnerabilities since at least Dec. 11. Indeed, the FTC’s post encourages companies to consult CISA’s guidance on mitigating them. What’s the use of this somewhat belated contribution to the conversation?

The reason is that the FTC has enforcement powers over private-sector wrongdoing that CISA doesn’t. By law, CISA’s remit is limited to the federal government and critical infrastructure, even though its alerts and guidance are used by others outside of those sectors too. Controversially, the young agency has little in the way of enforcement authority outside of the federal government; proposed expansions thereof still focus on critical infrastructure, not the private sector writ large. By contrast, the FTC has over 80 years of experience acting as the nation’s consumer protection watchdog. Federal law gives it the power to police and punish “unfair or deceptive acts or practices in or affecting commerce.” In recent years, the agency has relied on that authority to assume the mantle of Americans’ data-security defender. This application of its authority was challenged in court, but the agency prevailed. It’s brought multiple enforcement actions in the area of data security since then under both the “unfair” and “deceptive” prongs of the law. At this point, it’s well-established that shoddy cybersecurity is within the scope of the FTC’s enforcement powers.

In evaluating companies’ data security practices, the agency uses “reasonableness” as its touchstone. The trouble is that what’s “reasonable” or “unreasonable” is hard to pin down. Best practices change over time as both technology and threats evolve. A cybersecurity program that’s reasonable for a tiny company might be unreasonable for a huge one. And even otherwise comparable companies may not be similarly situated in a particular circumstance such as the Log4j issue: There’s a difference between companies that make the conscious decision not to patch Log4j and just accept the risk (to themselves and their customers), those that can’t patch for whatever reason, and those that don’t patch because they don’t even realize they use Log4j. The FTC’s blog post doesn’t draw these distinctions, but they should factor into any FTC analysis of whether to institute enforcement proceedings over Log4j lapses.

If a company has no way of knowing that the FTC considers a particular security practice “unreasonable,” that’s a problem for the agency. An important concept in U.S. law is that of “notice”: Everyone has the right to know, in advance, what conduct will subject them to government punishment, so they can conform their behavior accordingly. It’s not OK for the government to penalize conduct which it hadn’t put the public “on notice” was illegal.

That’s why the FTC must give notice of what business acts or practices are “unfair” under the law. It can do this by formally promulgating rules or by litigating on a case-by-case basis to establish an act or practice as “unfair.” In the cybersecurity context, companies targeted by the FTC have sometimes argued that the agency hadn’t given fair notice that their security practices were unreasonable. Sometimes the courts have rejected this argument, as in the FTC’s case against Wyndham Hotels, which had been hacked three times and had used security practices that the FTC had specifically denounced in its prior guidance and adjudications. Since the agency hasn’t batted a thousand in court, however, in the last few years it’s made an effort to improve its data security guidance to companies.

It’s this history that underlies the Jan. 4 missive, which the FTC’s chief technologist’s office posted to the “Tech@FTC” blog and disseminated on social media. I interpret this as the FTC’s attempt to put the country on notice that failure to patch the Log4j vulnerabilities risks subjecting a company to punishment. That said, as one cybersecurity law scholar observed, a blog post by the chief technologist’s office does leave something to be desired in terms of formality. That could leave the FTC open to the argument that the blog post doesn’t provide sufficient notice, unlike, say, official agency rulemaking. Nevertheless, should any company subsequently claim it didn’t know it was supposed to patch a flaw that’s typically been described in terms that “border on the apocalyptic,” the FTC can point to this warning, together with its other, formal past actions such as the Equifax proceeding, to refute that assertion.

#### Strong FTC penalty authority deters cyber attacks on critical infrastructure

Holland, 21 – Mackenzie, citing Edward Felten, professor of computer science and public affairs at Princeton and former chief technologist at the FTC. "Senators want FTC to enforce a federal data security standard," SearchSecurity, <https://searchsecurity.techtarget.com/news/252507933/Senators-want-FTC-to-enforce-a-federal-data-security-standard> -- Iowa

U.S. Senators want to empower the Federal Trade Commission to become a stronger protector and enforcer of consumer data privacy and security.

During the second in a series of hearings focused on the importance of federal standards for data privacy and security, the U.S. Senate Committee on Commerce, Science and Transportation listened to experts who recommended development of a data security standard for businesses that's enforced by the FTC. The first hearing explored the creation of a federal data privacy law as well as creation of a data privacy bureau within the FTC.

The call for federal data privacy and security standards follows attacks on critical infrastructure companies, including the 2021 attack on Colonial Pipeline. That attack, which caused fuel shortages, was cited by committee chair Sen. Maria Cantwell, D-Wash., as a reason necessitating federal standards.

Cantwell and Sen. Roger Wicker, R-Miss., have introduced two separate bills that would set U.S. privacy and security standards for businesses: the Consumer Online Privacy Rights Act and the Setting an American Framework to Ensure Data Access, Transparency and Accountability (Safe Data) Act. The legislation would also give the FTC and state attorneys general the ability to enforce the standards.

"We believe that these companies don't invest enough for the fact that they have oversight of our precious data and information," Cantwell said. "We know that a stronger FTC will help, but we need to give the FTC the resources they need to do their job."

Experts make data security standard recommendations

James Lee, chief operating officer at San Diego-based nonprofit Identity Theft Resource Center, echoed Cantwell's concern that the U.S. needs a federal data security standard and to better outline national cybersecurity best practices.

Lee said a federal data security standard should require companies to address small but preventable flaws that lead to data breaches, such as unpatched software, as well as minimize consumer data that can be collected and stored by companies. Additionally, Lee said stronger enforcement measures would be necessary for companies that fail to meet the data security standard.

"Without enforceable minimal standards, there are no broad incentives beyond trying to avoid headlines or post-breach litigation to get people to actually make broad organizational changes," Lee said.

"We need better enforcement," he said. The FTC is "best equipped to be that enforcement agency."

Indeed, Jessica Rich, counsel at law firm Kelley Drye and Warren LLP and former director of the FTC Bureau of Consumer Protection, said current law fails to set clear standards for data security or provide adequate remedies.

"Most of the FTC's data security efforts are based on the FTC Act, a law that leaves wide gaps in protection and doesn't authorize penalties for first-time violations," she said. "While there are sector-specific laws with a data security component, and half the states now have their own data security laws, it's a messy and confusing patchwork."

Rich recommended a standard that's scalable to different types and sizes of companies and the volume and sensitivity of the data they collect. Otherwise the law could impose requirements ill-suited and unattainable for small business, she said. Rich also supported data minimization incentives or requirements.

Rich said to ensure accountability and deterrence, the data security standard should authorize strong remedies such as civil penalties and redress to businesses that fail to meet the data security standard.

Edward Felten, Robert E. Kahn professor of computer science and public affairs at Princeton University and former chief technologist at the FTC, said the FTC currently doesn't have the tools it needs to address today's data security enforcement challenges.

To further empower the FTC, Felten voiced support for allowing civil penalties for first-time violations of certain statutes within the FTC Act, such as Section 5, which states that unfair or deceptive practices affecting commerce are unlawful. The lack of first-time penalties makes the FTC Act a "weak deterrent," he said.

Additionally, Felten said Congress could authorize data security rulemaking so the FTC can clarify what is expected of companies, as well as funnel additional resources to the FTC for data security and technology initiatives.

"The successful FTC of the future is one that has stronger authority, increased resources and greater technological capability," Felten said.

#### **The strength of FTC legal authority is the biggest global internal link**

Stokel-Walker, 1-10-22 – Chris, Wired journalist, “The FTC Wants Companies to Find Log4j Fast. It Won't Be Easy,” Wired, <https://www.wired.com/story/lo4j-ftc-vulnerability/> -- Iowa

Then, on January 4, CISA and the Federal Trade Commission issued a warning to US businesses. “When vulnerabilities are discovered and exploited, it risks a loss or breach of personal information, financial loss, and other irreversible harms,” the FTC wrote. “It is critical that companies and their vendors relying on Log4j act now, in order to reduce the likelihood of harm to consumers, and to avoid FTC legal action.”

The federal body said it wouldn’t hesitate to use its full legal authority “to pursue companies that fail to take reasonable steps to protect consumer data from exposure as a result of Log4j, or similar known vulnerabilities in the future.”

The statement shifted the calculus of risk and liability for businesses. Threatened with legal action, they feel compelled to act. The challenge, though, is finding out whether they’re affected.

Log4j’s ubiquity makes it difficult to know whether any individual organization is affected. First discovered in Minecraft, the Log4j vulnerability has since been found in cloud applications, enterprise software, and on everyday web servers. The program is an event recorder, monitoring simple actions, both routine and errors, and reporting them to system administrators or users. And Log4j is one small but common component in tens of thousands of products—many of which are then bundled up into bigger projects. So-called indirect dependencies—packages or parts of programs that businesses use as part of their IT solution that unwittingly use Log4j—are one of the biggest risks, reckons Google, with more than four in five vulnerabilities hidden several layers deep into the interconnected web of software.

“The FTC has decided to swing a big hammer,” says Ian Thornton-Trump, chief information security officer at threat intelligence firm Cyjax. But he doesn’t necessarily think it’s the right move, calling it “impudent” and an unhelpful way of ramping up the situation. Large companies are conscious of what they need to do when confronted by such an issue, Thornton-Trump believes, and don’t need the FTC breathing down their neck to make them act. “What you don't need is a federal government agency telling you what the priorities are for your business when they don't even know what your actual business risk might be,” he says.

Others disagree. “Part of the chaos is that all of these big supply chain issues can cause a disjointed effort at remediation,” says Katie Moussouris, founder and CEO of Luta Security, a cybersecurity consultancy. “So I do think the FTC’s pressure is important.”

The FTC’s bravado in compelling companies to act is the end result of a government department wanting to genuinely help businesses in the United States and abroad but constrained by the lack of political will to push through meaningful cybersecurity legislation that isn’t focused on particular, limited areas, such as health care or financial data, says Thornton-Trump. As a result, US cybersecurity policy is reactive, trying to fix issues once they arrive under penalty of legal action, rather than proactive, he argues. Nevertheless, the FTC’s move is an important one: Though the FTC is to date the only government body globally to issue a warning to companies to fix the problem or else, the Log4j vulnerability affects hundreds of millions of devices.

#### Cyber attacks on critical infrastructure go nuclear and are uncontrollable

Orlov 20 [Vladimir, 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.

#### Only robust penalty enforcement solves false ads – litigation and regulation fail

Tushnet and Carrier, 21 – Rebecca Tushnet is a Professor at Harvard Law School and former NDT Finalist. Michael Carrier is a Professor at Rutgers Law School. *An Antitrust Framework for False Advertising*, May, 106 Iowa L. Rev. 1841, p. Nexis – Iowa

The pharmaceutical industry has provided the setting for other examples of antitrust scrutiny of conduct that violates non-antitrust rules, particularly those relating to fraud. The Walker Process 121 line of cases holds that the fraudulent procurement of a patent or enforcement of a patent obtained by fraud can violate antitrust law. 122 Other cases involve the allegedly fraudulent [\*1869] listing of patents in the "Orange Book," 123 an annual compilation of drugs and their associated patents. 124 And courts have recognized antitrust liability when a brand company makes "repeated and allegedly false patent descriptions" to the FDA. 125

Despite these cases, one could conceivably argue that antitrust should not apply to actions that are also governed by a separate regulatory regime. In Verizon Communications v. Law Offices of Curtis V. Trinko, the Supreme Court indicated that where another regulatory regime is guaranteeing competition, there may not be a need for antitrust enforcement. 126 That case can only be fully understood, however, in relation to the industry in which it arose. The Court in the case was evaluating the Telecommunications Act, which provides the Federal Communications Commission ("FCC") with general - and effective - regulatory authority over the industry, including its competitive structure (e.g., restrictions on concentrated ownership and must-carry requirements). 127

Other settings require more robust antitrust enforcement. For example, the FDA has very specific authority over drugs and medical devices, but it does not pervasively regulate industry structure in the way that the FCC does. Instead, the FDA has concluded "that issues related to ensuring that marketplace actions are fair and do not block competition would be best addressed by the FTC, which is the Federal entity most expert in investigating and addressing anticompetitive business practices." 128 Much more similar to [\*1870] the FDA than FCC, false advertising regulation lacks the pervasive control and monitoring, including reporting requirements, of telecommunications law. 129

False advertising litigation cannot effectively stand in for the antitrust function. False advertising, unlike the FCC's jurisdiction, is broad rather than deep: it covers a wide variety of competitive situations, from mouthwash to specialized airline components, but only by barring falsity and deception rather than by pervasively dictating market structure. Of critical significance, moreover, false advertising law is itself underenforced. The FTC has substantial resource constraints. And consumers themselves are rarely able to sue for the harms they suffer. Consumer contracts typically contain mandatory arbitration provisions, making schemes like AT&T's market-shaping deception harder to fight. As a result, there is no "false advertising regime" that effectively fosters competition and negates the need for antitrust enforcement. 130

#### **Regs can’t address market-wide harms from false ads, only antitrust can**

Tushnet and Carrier, 21 – Rebecca Tushnet is a Professor at Harvard Law School and former NDT Finalist. Michael Carrier is a Professor at Rutgers Law School. *An Antitrust Framework for False Advertising*, May, 106 Iowa L. Rev. 1841, p. Nexis – Iowa

[\*1844] False advertising law allows consumers to receive some redress for the money they paid for "unlimited" data that wasn't, 5 but there's no obvious remedy for the damage AT&T caused to the market as a whole. Antitrust law has been kneecapped by the courts and thus is powerless to act. In short, the law's neglect of the injuries caused by false advertising threatens structural harm to competitive markets.

In this Essay, we address these problems. We do so by focusing on the actors most likely to harm the market: monopolists and attempted monopolists. These actors are a numerically small percentage of businesses (and of false advertising defendants), but they can do great harm. Our emphasis on monopolists and attempted monopolists addresses courts' concerns of overbroad enforcement, preventing false advertising from morphing automatically into an antitrust violation. And it carves out a critical role for antitrust while embracing - rather than neglecting - antitrust's partner in fighting unfair competition, false advertising law.

We begin by introducing the laws of antitrust and false advertising, explaining the regimes' objectives and methods. We then survey the antitrust caselaw, critiquing three approaches courts considering false advertising claims have taken. Finally, we introduce our antitrust framework for false advertising claims. At the heart of the framework is a presumption that monopolists engaging in false advertising violate antitrust law, with that presumption rebuttable if the defendant can show that the false advertising was ineffective. The framework also applies to cases of attempted monopolization by incorporating factors (falsity, materiality, and harm) inherent in false advertising law, along with competition-centered issues on targeting new market entrants and entrenching barriers to entry. To illustrate how our framework should work, we apply it to an important area: advertising for biosimilars, which are pharmaceutical products with a substantial and growing role in treating numerous diseases.

False advertising that exacerbates monopoly power has been dismissed by antitrust law for too long. This Essay seeks to resolve the contradiction in the law by showing how false advertising threatens the proper functioning of markets.

#### **POA against targeted industries triggers the link but doesn’t solve the aff**

TINA, 1-5-22 –Truth in Advertising, Inc. (TINA.org) is a 501(c)(3) nonprofit dedicated to empowering consumers to protect themselves and one another against false advertising and deceptive marketing. “Deceptive ad Trends to be Wary of in 2022,” <https://www.truthinadvertising.org/deceptive-ad-trends-to-be-wary-of-in-2022/> -- Iowa

Deceptive Income Claims

Throughout October 2021, the FTC used its penalty offense authority to put a number of industries on notice, informing them of certain truth-in-advertising laws and of the agency’s ability to seek big financial penalties against those who then knowingly violate those laws. Among those industries targeted was the multilevel marketing industry. Since our founding in 2012, TINA.org has catalogued thousands of examples of MLMs using deceptive income claims to promote the “business opportunity,” despite the fact that the FTC has said most people who join legitimate MLMs make little or no money (which is why MLMs should generally avoid making any income claims). Before the FTC sent notices reminding the MLM industry to stay away from exaggerated or false earnings claims in its recruitment efforts, TINA.org sent a letter to the FTC in June urging it to implement a penalty offense program directed at that very industry. We attached a list of 668 MLMs; the FTC ended up sending notices of penalty offenses to 638 of them. At as much as $43,792 per violation, if the message is not received, some MLMs could be facing some hefty financial penalties in 2022.

#### Only broad POA saves the FTC from total destruction

Chopra and Levine, 21 – Rohit Chopra was a Federal Trade Commissioner and is now head of the Consumer Financial Protection Bureau (CFPB). Samuel A.A. Levine is Acting Director of the Bureau of Consumer Protection. *The Case for Resurrecting the FTC Act’s Penalty Offense Authority*, Social Science Research Network (SSRN), Feb 16 last revised, originally published 11/3/20, [https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3721256](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3721256&download=yes) – Iowa

Deploying the Penalty Offense Authority should be part of a broader strategy to resurrect the FTC as a vigorous check against corporate malfeasance. This article has detailed how the authority can be used to notice whole industries of unlawful practices, and to seek remedies that not only reverse the effects of wrongdoing but also deter others from crossing the line. We have identified five areas where the Commission has already condemned practices that can be designated as penalty offenses. Going forward, as the Commission condemns new forms of misconduct, we believe it should include in its orders clear findings that can be served on other market participants.

In addition to increasing the agency’s ability to deter and correct wrongdoing, resurrecting the Penalty Offense **A**uthority would mitigate the ongoing gamesmanship around Section 13(b), showing the marketplace that the FTC has more than one trick up its sleeve, regardless of how the Supreme Court rules.

The Commission’s overwhelming reliance on Section 13(b) is of recent vintage. In the 1970s, following widespread dissatisfaction with “scandalously weak” no-money orders,174 Congress armed the Commission with strong tools to meaningfully deter widespread lawbreaking. These tools include rulemaking powers backed by civil penalties, the ability to seek damages under Section 19, and the Penalty Offense Authority described here. However, these powers were largely abandoned after James C. Miller III took over the FTC in 1981, as the Commission shifted its focus to halting scams using Section 13(b).

The takeover and subsequent gutting of the Federal Trade Commission by Chairman Miller is an underappreciated milestone in our nation’s economic history.175 By shifting attention and resources away from scrutinizing emerging business practices that pose harm to households and honest businesses, Miller and his lieutenants architected a new paradigm for corporate oversight. The FTC abandoned its former role and began to duplicate the role of criminal law enforcers who tackle fraud rings, but without the authority to seek any criminal sanctions. The Commission’s new emphasis on shutting down “illegitimate” businesses created the guise of an active agency, when, in reality, it became increasingly irrelevant to commercial regulation across many sectors of the economy.

Since the Miller era, the Commission had essentially ceded its role as the government’s analytical engine of emerging commercial practices. The result has too often been an agency that is disconnected from pressing market problems. In recent decades, the Commission has failed to tackle some of the worst abuses facing consumers, ranging from subprime mortgage lending to predatory for-profit colleges. By 2010, as Congress stripped key authorities from the Commission, industries actively lobbied to remain under FTC jurisdiction, 176 an effort currently being replicated by tech titans in the privacy arena.177 This does not reflect well on the agency’s credibility as a watchdog.

For the architects of this ideological project to weaken the FTC, the current judicial threats to Section 13(b) could prove to be the most striking blow yet. They have long argued that Section 13(b) should be used only in cases involving “true fraudsters,”178 and they have offered a detailed blueprint to those wishing further limit the Commission’s remedial authority.179 Should they succeed, this would represent the culmination of their decades-long project to defang this once-storied agency, conceived of by Louis Brandeis to be a strong check on corporate power.

But if the FTC is rendered toothless, this is by choice. The agency can shed its self-inflicted paralysis by using the dormant powers granted by Congress. Regardless of how the Supreme Court rules, the Commission must close the chapter on its overreliance on Section 13(b), and deploy a broader set of tools to meet its mission. By deploying these tools, the Commission can reemerge as a vigorous watchdog, detecting and deterring systemic harm instead of playing whack-a-mole against small scams. Adopting this approach is essential to regaining the public’s confidence and realizing Brandeis’s vision of an agency that protects the public from abuse and misuse of corporate power.

#### Any approach but antitrust is incoherent – presumption against monopolists solves

Tushnet and Carrier, 21 – Rebecca Tushnet is a Professor at Harvard Law School and former NDT Finalist. Michael Carrier is a Professor at Rutgers Law School. *An Antitrust Framework for False Advertising*, May, 106 Iowa L. Rev. 1841, p. Nexis – Iowa

Federal law presumes that false advertising harms competition. Federal law also presumes that false advertising is harmless or even helpful to competition. Contradiction is not unknown to the law, of course. This contradiction, though, is acute. For not only are both regimes at issue designed to protect competition, but they are both enforced by the same agency: the Federal Trade Commission, which targets "unfair competition" through antitrust and consumer protection enforcement.

Courts' treatment of false advertising in antitrust cases makes no sense. While courts have reasonably evidenced concern that not all false advertising violates antitrust law, the remedy is not to abandon the false advertising/antitrust interface. Instead, the solution is to focus on the actors most likely to harm the market: monopolists and attempted monopolists.

This Essay proposes an antitrust framework for false advertising claims. It introduces a presumption that monopolists engaging in false advertising violate antitrust law and a rebuttal if the false advertising is ineffective. The framework also applies to attempted monopolization by incorporating factors such as falsity, materiality, and harm inherent in false advertising law, along with competition-centered issues like targeting new market entrants.

Antitrust has dismissed false advertising that entrenches monopoly power for too long. This Essay seeks to resolve the contradiction in the law by showing how false advertising threatens the proper functioning of markets. Such an approach promises benefits for false advertising law, antitrust law, and consumers.