# 1AC

### 1

#### The Advantage is Innovation

#### The Ninth Circuit’s Decision in Qualcomm has barred antitrust from cases involving Standard Essential Patents (SEPs). That gives patent holders undue bargaining leverage against implementers.

Sullivan 20 [Sullivan & Cromwell LLP, Leading Firm in Business Law “Ninth Circuit Holds That Qualcomm’s Patent Licensing Program Does Not Violate U.S. Antitrust Law”. 8/12/20. https://www.sullcrom.com/files/upload/sc-publication-ninth-circuit-holds-qualcomm-patent-licensing-program-does-not-violate-us-antitrust-law.pdf]

The Ninth Circuit’s decision, unless modified by the Supreme Court, affirms Qualcomm’s SEP licensing model for OEMs (and its refusal to license rival chipmakers), at least with respect to any challenge under U.S. antitrust laws. Because Qualcomm’s model has driven the cellular modem licensing and sale landscape for chip suppliers and handset makers alike, the court’s decision will likely quiet concerns on the part of some that the district court’s decision would upend that market, although it perhaps makes it less likely that the market will see increased competition or that chip prices will drop as may have been the case if Judge Koh’s injunction had been upheld.

Although the court confirmed that an SEP holder has no antitrust duty to deal with rivals outside the limited Aspen Skiing exception, the Ninth Circuit left open the possibility that an SEP holder’s FRAND commitments may obligate it to deal with its rivals.39 Importantly, however, the Ninth Circuit clarified that a company’s breach of its FRAND commitments does not amount to anticompetitive conduct in violation of the Sherman Act. Instead, the remedy for such conduct lies in contract law. Moreover, the court’s decision to vacate as moot the district court’s summary judgment decision—which found that Qualcomm was required by its FRAND commitments to license rival chipmakers—removes what some had considered to be persuasive judicial authority in the U.S. supporting a claim that FRAND requires licensing at all levels of a product distribution chain which implement a standard. This is noteworthy for SEP holders because it returns U.S. jurisprudence to the status quo, and at least one court in the Eastern District of Texas interpreted a comparable FRAND commitment as not requiring a SEP holder to license all comers at any level of the supply chain. This issue continues to be litigated in the U.S., notwithstanding the Department of Justice Antitrust Division general view that the market, not FRAND, should determine license structures.

The court’s refusal to force licensing at the chip level (rather than the OEM level) also may ease concerns that patent-exhaustion considerations could be used to limit SEP licensors’ ability to maximize profits if licenses were required at the chip level. The Ninth Circuit confirmed that royalty rates are not required to be set strictly using the SSPPU and recognized that “OEM-level licensing is now the industry norm.”40 The Ninth Circuit also recognized that “[t]here are good reasons for SEP owners to structure their licensing programs to license end-user products.”41 The court’s findings appear consistent with current flexibility in structuring FRAND licensing programs.

The Ninth Circuit’s decision also recognizes that royalty rate determinations, and particularly the determination of a FRAND rate, are an issue that sounds in patent law, not antitrust law. The court “decline[d] to adopt a theory of antitrust liability that would presume anticompetitive conduct any time a company could not prove that the ‘fair value’ of its SEP portfolios corresponds to” what the market is willing to pay for those SEPs in royalty rates.42 Arguably, the Ninth Circuit’s decision will impact negotiation power between patent owners and technology implementers by clarifying the circumstances under which patent licensing conduct will give rise to antitrust liability.

Finally, the Ninth Circuit’s decision is noteworthy beyond its application to SEP licensing because it recognizes and demonstrates that courts should be reluctant to ascribe antitrust liability based on conduct occurring in a dynamic, rapidly evolving market—a characterization that will apply to many existing and emerging technology markets.

#### Three internal links

#### 1 – SEP holders refuse to license their patents on fair, reasonable, and non-discriminatory (FRAND) terms– that kills innovation and locks SMEs out of emerging tech markets

* Note – Refusal to license and rate hikes are encompassed in the concept of patent hold-up

FTC 18 [Federal Trade Commission, Signed by ACT, Auto Alliance, CCIA, HTIA, NRF, SIIA Organizations. “Standards, Licensing, and Innovation: A Response to DOJ AAG’s Comments on Antitrust Law and Standard-Setting”. 08/2018. https://www.ftc.gov/system/files/documents/public\_comments/2018/08/ftc-2018-0055-d-0031-155033.pdf]

2. Standardization Gives Rise to Patent Hold-Up

As the Antitrust Division, other federal agencies, and U.S. courts have long recognized, patent hold-up creates risks to competition.17 Characterizing hold-up as a “unilateral” problem that antitrust law should not be concerned about ignores that the power to hold up arises from concerted multilateral action by participants, often competitors, in a standard-setting organization agreeing on specific technologies to use in the industry. Standardization forecloses alternatives that would otherwise compete in the marketplace, and the FRAND commitment is intended to be a constraint on market power that standardization can create. Efforts by patentees to evade promises they made to license on FRAND terms comprise the abuse of monopoly power that the FRAND commitment is intended to limit. 18 Such unearned monopoly power derives not necessarily from the patentee’s “superior skill, foresight, and industry,” 19 but may derive instead from the fact that it is impossible to design around SEPs while maintaining compliance with the standard, creating a “lock-in” effect.20

Before the adoption of a standard, alternative technological solutions generally exist to provide a particular functionality for which the standard-setting process seeks a uniform, market-wide solution.21 Companies with patents that may cover these alternative solutions compete vigorously for inclusion of their preferred technologies into each standard. Once a standard is set, ex ante competition ceases. Patents that cover the chosen technology become essential because they must be used to comply with the standard. And once a standard achieves commercial acceptance, compliance with the standard becomes a matter of commercial necessity, as failing to comply with the standard would render a product incompatible with other companies’ products. This creates a “lock-in” effect, whereby companies that make or use standard compliant products must use the SEPs that are incorporated into the standards that they implement.22 The degree of lock-in reflects what may be the prohibitive costs of switching away from the standardized technology.

Incorporation of a patent into a standard therefore changes the balance of power between patent holders and prospective licensees dramatically, as the Ninth Circuit explained in Microsoft Corp. v. Motorola, Inc.:

[O]nce a standard becomes widely adopted, SEP holders obtain substantial leverage over new product developers, who have little choice but to incorporate SEP technologies into their products. Using that standard-development leverage, the SEP holders are in a position to demand more for a license than the patented technology, had it not been adopted by the SSO, would be worth. The tactic of withholding a license unless and until a manufacturer agrees to pay an unduly high royalty rate for an SEP is referred to as “hold-up.”23

The SEP holder’s strengthened bargaining position after adoption of a standard is directly attributable to the elimination of alternatives to the SEP resulting from the adoption of a standard. Because license negotiations typically do not take place until after a standard has been adopted, when the SEP holder is no longer competing to have its technology included in the standard, the prospective licensee is “at the patentee’s mercy.”24 Prospective licensees therefore may be willing to pay a much higher royalty for use of the patented technology than they would have been willing to pay ex ante, when the SEP holder faced competition from other technologies. Further, while large corporations familiar with SEP licensing may be able to absorb the cost of an unreasonable license or seek redress in court at significant cost to their own innovative efforts, the same opportunities may not be available to small and medium enterprises. These innovators may be forced to abandon business plans in standard-dependent markets entirely.

As a result, the Antitrust Division has recognized that, unless constrained, a SEP holder can exploit its unearned market power to obtain unfair licensing terms, including access to a licensee’s patents at unreasonable prices or supra-competitive royalties that are significantly higher than the SEP holder could have obtained before its patent was incorporated into the standard.

#### FRAND process will collapse now because firms follow Qualcomm – shreds competition in SEP Markets

Hovenkamp 20 [Herbert, James B. Dinan University Professor, University of Pennsylvania Law School and The Wharton School. ‘’FRAND and Antitrust’’. <https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3095&context=faculty_scholarship>]

While the FRAND process has been highly productive, it is also fragile. Firms are tempted to make commitments at the beginning when the incentive to join is large, but renege on them later when they can profit by doing so. At least in this particular case, private FRAND enforcement had not worked very well. Qualcomm had been able to violate FRAND commitments in order to exclude rivals and obtain higher royalties than FRAND would permit, largely with impunity. Other firms will very likely follow Qualcomm’s lead. If that happens the FRAND system will fall apart, doing irreparable injury to the modern wireless telecommunications network or, at the very least, diminishing the leadership role of the United States in preserving effective network competition.

#### SMEs are the lynchpin of emerging tech innovation

Corl 19 [Eric, Business News Expert, Entreprenuer, Founder and CEO of IdeaBuyer. “How Startups Drive the Economy”. 3/14/19. https://medium.com/@ericcorl/how-startups-drive-the-economy-69b73cfbae1]

According to a 2016 report from the Kauffman Foundation, transformation startups have been launched at a faster rate in recent years but still has a way to go.

These “high” growth firms make up just 15% of all companies. But they contribute an estimate of 50% of total jobs created. These young companies comparably invest more in research and development (R&D) than older ones.

The focus of this article is on Transformational startups.

The Big Small Impacts

Startups may be small. But they create ripples in the economy that change people’s way of living.

Here are the ways startups disrupt the economy and forces it to evolve, taking technology one -or several steps- higher.

1. Advance Technology

Older companies or incumbents are more likely to invest in R&D on existing technologies and incremental innovation. While startups are more focused on new technologies and cutting-edge innovation.

Free from a multilayered corporate bureaucracy, startups are more agile and able to build an idea into a product and improve it upon consumer demand with faster decision-making communications. Its high stakes deeply motivate its employees to do whatever it takes to succeed.

Giant companies like Google and Microsoft often acquire startups and use their size and distribution channels to improve the innovation and boost its sales.

However, a member of Harvard’s Labor and Worklife Program, Vivek Wadhwa argues that “when technology’s top guns join these companies, they seem to make a smaller impact than those that don’t get hired.” He then advised that startups must be armed with seed financing in order for the economy get more technological innovation.

2. Open New Markets

Startups create new markets or completely transform old markets by introducing products that change the world. Giants today like Apple, Facebook and Google were once small but ambitious startups.

New technologies often create new opportunities that startups take advantage of. Startups then create a massive value over mature businesses, inspiring competition and disrupting the economy to evolve.

However, not all startups succeed. According to James Surowiecki of MIT Technology Review, the reason behind this is the increased power of established incumbents. Though incumbents have been toppled before, the American industry has grown more concentrated over the last 30 years.

3. Boost Production of Goods and Services

According to Bryan Ritchie and Nick Swisher of IDEA Center, startups disproportionately have higher technology. This drives up production of goods and services.

In a 2017 report by the Center for Economic Studies at the US Census Bureau, they have found that firms that have a high growth output are disproportionately young and “makes disproportionate contributions to output and productivity growth.”

In another paper published on 2011 by Small Business Administration, startups were discovered to generate more revenue with the same number of capital inputs than older companies.

4. Increase Employment

Startups create jobs. These “high-growth” firms are companies that add jobs at a rate of 25 plus percent.

Wadhwa states, “Without startups, there would be no net job growth in the US economy. From 1977 to 2005, existing companies were net job destroyers, losing 1 million net jobs per year. New businesses in their first year added an average of 3 million jobs annually.”

In a 2017 report by the Progressive Policy Institute, the private sector job growth is significantly higher where the startup activity is high. In contrast, regions with few startup activity experience less than half the job growth.

5. Direct Local Impacts

Startups also have a direct change on the cities where they are located such as how Microsoft has transformed Redmond and Google has changed Mountain View California. They bring in wealth and a large inflow of graduates and experienced professionals from other locations who are looking for job opportunities.

Startups are a Driving Economic Force

Startups are engines of growth. To avoid economic stagnation, methods must be sought to foster competition and assist transformational entrepreneurs.

While it is important to get support in a federal level, the effort must be focused in a local level. Cities need to foster programs that encourage entrepreneurship. It is absolutely critical for growth at a local and national level and legislative and political motives can no longer take entrepreneurs into account as an after-thought.

Removing barriers. Facilitating connections. Empowering startups. These are just the few ways for civic leaders to give a better edge to entrepreneurs.

Over the years, I’ve gotten more and more involved in advocating for other entrepreneurs and I’ve been introduced to some great organizations. For one, the SBE Council (http://www.SBECouncil.org) is doing a wonderful job on the federal level advocating for entrepreneurs and small businesses to make sure our voices are heard. Please follow them and support them online.

The Small Business Administration is also doing great work with their main street leaders program to connect local businesses to Washington, DC. If you have a business, they want to hear your voice.

Remember, startups are the driving force behind our economy — we must advocate for the entrepreneurs behind them and continue to foster innovation.

#### 2 – Excessive sham litigation plagues standard patent disputes – only the federal legal clarity of the plan solves

Hovenkamp 19 [Herbert, James B. Dinan University Professor, University of Pennsylvania Law School and The Wharton School. “FRAND and Antitrust”. 9/2019. https://awards.concurrences.com/IMG/pdf/2.\_frand\_and\_antitrust.pdf?55742/742050234fc2871a2db38c61d1e7936e388e6cc9]

Abuses of the Judicial Process

Should the owner of FRAND encumbered patents be accountable under the antitrust laws for the way it employs judicial processes? For example, suppose that the owner of a FRAND patent seeks an injunction against a manufacturer of a good that employs the patent and participates in the standard. Patentees have a statutory right to obtain an injunction against proven infringers.193 As a result, seeking injunctive relief from a court should not ordinarily be an antitrust violation.

Nevertheless, there are important qualifications. If someone files a suit that no reasonable litigant would have brought with the expectation of success, then antitrust liability can attach. In such cases the litigation plaintiff’s expectation of success comes not from winning the lawsuit, but rather from depleting the defendant’s assets, delaying its market entry, or otherwise injuring it in ways unrelated to the outcome of the litigation.

The grandparent of these cases is Walker Process Equip., Inc. v. Food Mach. & Chem. Corp.194 The patentee had a patent that it knew to be unenforceable under the statutory on sale bar,195 but it attempted to exclude a competitor from the market anyway via a patent infringement suit. The Walker Process case applied the so called “sham” litigation exception that holds that the filing of a law suit loses its First Amendment protected status if the lawsuit is a “sham,” which means that it was filed without a realistic prospect of success from the litigation itself, but rather to intimidate, harass, or deplete the resources of the litigation defendant.196

One important precondition to the sham litigation exception is that existing law be sufficiently “settled” that a lawsuit filed in conflict with it should be regarded as “objectively meritless.”197 That is, a reasonable person in the plaintiff’s position should have known that the lawsuit would not succeed. For example, if there is a conflict in the Federal Circuit Courts of Appeal respecting a particular issue, a plaintiff should be entitled to convince the appellate courts to apply one interpretation rather than the other one.198 Issues of first impression or those that could reasonably come out either way can of course be the subject of litigation.

There is no obvious reason that the sham litigation rule should not apply in the FRAND context, and under these same constraints. Once it has become a matter of settled law that a SEP owner is not entitled to an injunction under a given set of circumstances – that is, that a knowledgeable person would realize that there was no genuine prospect of relief -- then further lawsuits under those circumstances may give rise to antitrust liability.199 If the lawsuit is plainly in violation of an enforceable contract obligation, Walker Process liability should be appropriate. On the other hand, if the issue remains open to legal doubt, then filing a lawsuit is appropriate, even if the suit is ultimately unsuccessful.

Sham litigation establishes the conduct element of an antitrust offense. In order to establish an antitrust violation, the challenger would still have to make out the other elements of an antitrust cause of action – namely, power and unreasonable exclusion for §2 cases, or a restraint of trade for §1 cases. 200

For example, once the FRAND obligation for a patent or set of patents has been established to require licensing to all implementers operating on the standard, a firm that files infringement lawsuits seeking injunctions against firms simply because they are product market competitors should generate the conduct basis for antitrust liability. While this road to antitrust liability might seem narrow, it becomes broader as litigation clarifies issues so that they can be regarded as settled.

#### Just the threat of sham injunctions stifles innovation by hiking licensing rates and legal costs

Wood 13 [Chris Wood and Joseph Kattan, partners in the Antitrust and Trade Regulation practice of Gibson, Dunn & Crutcher LLP. “Standard-Essential Patents and the Problem of Hold-Up”. 12/13/13. http://awa2014.concurrences.com/IMG/pdf/standard\_essential\_patent\_kattan-wood.pdf]

The threat of an injunction is an extraordinarily powerful weapon when asserted by a SEP holder, as the potential licensee faces the prospect of its product being excluded from the market. As one federal court framed the issue, “[i]t would seem clear that a negotiation where one party … must either come to an agreement or cease its sales … fundamentally places that party at a disadvantage.”51 Similarly, the European Commission has noted that “the threat of injunction, the seeking of an injunction or indeed the actual enforcement of an injunction granted against a good faith potential licensee, may significantly impede effective competition by, for example, forcing the potential licensee into agreeing to potentially onerous licensing terms which it would otherwise not have agreed to.”52 As a result, a rational implementer faced with an injunction threat may well conclude that paying an unreasonable royalty is less risky than fending off infringement litigation.53

The use of injunctive relief against willing licensees, or the threat of seeking such relief, is fundamentally incompatible with the FRAND promise. Injunctive relief is an extraordinary remedy that is available only where a patent holder would be “irreparabl[y]” harmed due to a lack of available monetary relief.”54 By contrast, a SEP holder that makes a FRAND commitment agrees to license its SEPs to any standard implementer willing to pay a FRAND compliant royalty, thereby acknowledging that monetary compensation constitutes adequate remuneration for its SEPs.55 As Judge Posner has observed, “[b]y committing to license its patents on FRAND terms, [the SEP holder] committed to license … to anyone willing to pay a FRAND royalty and thus implicitly acknowledged that a royalty is adequate compensation for a license to use that patent.”

Some authors have argued that the language of FRAND commitments “cannot be read to suggest abdication of injunctive relief.”57 But the plain meaning of the FRAND language used by leading SSOs requires that SEP holders grant a license to every willing licensee. For example, the bylaws of the U.S.-based IEEE, which is responsible for the development of the Wi-Fi standard for wireless networking, state that a FRAND commitment must provide “that a license for a compliant implementation of the standard will be made available to an unrestricted number of applicants on a worldwide basis …. under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination.”58 In analyzing the virtually identical FRAND commitment of the International Telecommunications Union (“ITU”), the U.S. Court of Appeals for the Ninth Circuit determined that “[t]his language admits of no limitations as to who or how many applicants could receive a license.” 59 Similarly, the Intellectual Property Rights (IPR) Policy of ETSI, which is responsible for the development of the 3G and 4G telecommunications standards, while framed in different language, also requires that FRAND commitments guarantee a license to every willing licensee. It requires “an irrevocable undertaking in writing” to grant irrevocable licenses on FRAND terms to “manufacture, including the right to make or have made customized components and sub-systems to the licensee’s own design,” “sell, lease, or otherwise dispose of equipment so manufactured,” “repair, use, or operate equipment,” and “use methods.”60 By mandating a license for every potential application of a patent— from manufacture to sale to lease to use or repair—this policy contemplates that the FRAND commitment exclude no potential licensee that is ready to take a license on FRAND terms.

Given that injunctions are designed to provide a remedy where monetary compensation cannot, injunctions should be reserved for the limited circumstances in which monetary damages are an insufficient remedy for patent infringement.61 If a standard implementer is either unwilling or unable to pay a judicially-determined FRAND royalty, or is outside the court’s jurisdiction so that monetary relief could not be enforced, monetary compensation may not be an adequate remedy, in which case an injunction should be available. Whenever the SEP holder is able to secure monetary compensation, however, the threat of injunctive relief serves no purpose other than to give the SEP holders leverage to extract royalties above the FRAND levels that they contractually agreed to accept.

#### 3 – Agency flip-flopping triggers mass investment uncertainty and confirms fears that enforcement will switch on the president’s whim

Syrett 19 [Timothy, partner at WilmerHale, is an intellectual property and antitrust litigator. “The FTC’s Qualcomm Case Reveals Concerning Divide with DOJ on Patent Hold-Up”. 6/28/19. https://www.ipwatchdog.com/2019/06/28/ftcs-qualcomm-case-reveals-concerning-divide-doj-patent-hold/id=110764/]

The DOJ’s turn away from its long-held position on the risks of patent hold-up is a cause for serious concern.

First, it is bad policy. In explaining the DOJ’s about-face, Delrahim has referred to a “so-called ‘hold-up’ problem in the context of SSOs” and contended that concerns with hold-up “rely on models devoid of economic or empirical evidence that hold-up is a real phenomenon.” But the DOJ’s prior recognition of the risks of patent hold-up was well supported.

U.S. courts have long recognized that SEPs pose a hold-up threat. In 2007, for example, the Third Circuit observed that “[t]o guard against anticompetitive patent hold-up, most [standards development organizations] require firms supplying essential technologies for inclusion in a prospective standard to commit to licensing their technologies on FRAND terms.” Broadcom Corp. v. Qualcomm Inc., 501 F.3d 297, 313 (3d Cir. 2007). More recently, the Ninth Circuit explained that “[t]he development of standards . . . creates an opportunity for companies to engage in anti-competitive behavior” and that “[u]sing that standard-development leverage, the SEP holders are in a position to demand more for a license than the patented technology, had it not been adopted by the SSO, would be worth.” Microsoft Corp. v. Motorola, Inc., 795 F.3d 1024, 1031 (9th Cir. 2015); see also, e.g., Ericsson, Inc. v. D-Link Sys., Inc., 773 F.3d 1201, 1209 (Fed. Cir. 2014) (“SEPs pose two potential problems that could inhibit widespread adoption of the standard: patent hold-up and royalty stacking”).

As to the economics of patent hold-up, the DOJ observed in a 2015 business review letter that the “economic bargaining model underlying claims of hold-up has been studied extensively and applied to the standard-setting context,” citing scholarship dating back decades. That conclusion echoed the views of the DOJ and FTC in their 2007 report that patent hold-up is simply a “variant of the classic ‘hold-up problem’.” The DOJ also noted in its 2015 letter that “litigated cases demonstrate the potential for hold up when owners of RAND-encumbered standards-essential patents make royalty demands significantly above the adjudicated RAND rate” and provided examples where licensors’ demands were on the order of about 170 to 230 times what courts determined were RAND rates.

Recognition of the dangers of hold-up is thus well supported as a matter of law and economics. To be sure, if competitors collude in an SSO to fix the terms on which they will license technology, antitrust enforcement would be appropriate. But simply because one can envision the possibility of an alternative form of anticompetitive conduct relating to standard setting does not mean that the DOJ should simply ignore the well-documented existence of another form of harm.

Second, the DOJ’s abrupt shift away from over a decade of guidance on hold-up creates uncertainty for the many industries that rely on standards. While the shift in policy has been cast as being motivated by a concern for fostering innovation, it threatens to have the opposite effect. Companies planning investments in standardized products now face greater uncertainty about whether they can count on established rules, particularly as articulated in the DOJ’s business review letters, to safeguard their ability to license SEPs on FRAND terms.

Third, that a change in administration has led the DOJ to turn away from a long-held, bipartisan approach plays into the perception that antitrust enforcement is increasingly a political tool. While there may be higher profile examples of the politicization of antitrust enforcement, any step that suggests that a change in administration, not law and economics, will lead to wholesale departure from existing antitrust policy is troubling.

#### Tech investment certainty is the maker or breaker of broader innovation– only the plan stabilizes patent and antitrust certainty

Michel 17 [Hon. Paul R. Michel, Former Chief Judge, U.S. Court of Appeals for the Federal Circuit; Matthew J. Dowd, founder Dowd PLLC, "THE NEED FOR “INNOVATION CERTAINTY” AT THE CROSSROADS OF PATENT AND ANTITRUST LAW", April 2017, [https://www.competitionpolicyinternational.com/wp-content/uploads/2017/04/CPI-Michel-Dowd.pdf](https://www.google.com/url?q=https://www.competitionpolicyinternational.com/wp-content/uploads/2017/04/CPI-Michel-Dowd.pdf&sa=D&source=hangouts&ust=1631479189098000&usg=AOvVaw15b1X_q2CCXmXzm69Ur4_h)]

Innovation has long been the driving force of the U.S. economy.2 From the early days of our nation, inventors played a pivotal role in creating wealth for a growing nation, and this innovation continues today. Quantum computing research being funded by Google, IBM, Intel, and Microsoft; Genetic engineering, such as CRISPR; Autonomous vehicles, such as Otto’s self-driving trucks: The nation’s continued success in innovation is critical for maintaining the United States as an economic leader.

Successful innovation requires the proper environment. Innovators need intellectual capital, an educated workforce, and access to financial capital. These resources enable innovators to conduct the research and development and to optimize products for the commercial marketplace.

Equally important is a sufficient degree of what we call “innovation certainty.” Innovation certainty considers those legal, regulatory, and political factors that affect the degree of risk. The lower the degree of innovation certainty, the less hospitable the system is for innovators and investors. The less stable the legal and political rules, the more inimical the jurisdiction is to the investors who ultimately finance the innovative work.

During the past ten years, innovation certainty in the United States has decreased dramatically, and the decrease is directly attributable to two general trends: The destabilization of patent law, and the increased uncertainty in antitrust law. Both patent law and antitrust law, when properly implemented, contribute to an optimal level of innovation certainty. Patent law incentivizes innovation by awarding exclusive rights, thereby encouraging investment in and public disclosure of inventions.3 Antitrust law incentivizes innovation by maximizing competition in a free marketplace and allowing startup innovators to disrupt markets and avoid monopolies created by market power. Working within these legal regimes, private firms innovate and commercialize. They also create efficient transaction mechanisms, such as standard setting organizations (“SSOs”) and FRAND (“fair, reasonable, and non-discriminatory”) licensing agreements for standard essential patents (“SEPs”), so that innovators and their investors can efficiently obtain a return on their capital.

#### Winning the commercial tech innovation race solidifies military overmatch BUT the lead is razor-thin now

Molling 18 [Christian, research director of DGAP, German Council on Foreign Relations. “Defense Innovation and the Future of Transatlantic Strategic Superiority: A German Perspective”. 3/23/18. https://www.gmfus.org/news/defense-innovation-and-future-transatlantic-strategic-superiority-german-perspective]

Technological superiority is key for the West’s military power. But the reality of how to maintain this superiority is changing. Instead of innovation in defense technology coming predominately from national programs linked to the military, innovation is now increasingly generated by the private sector and takes place around the globe. The competition of commercial companies for their consumers has also led to shorter innovation cycles, especially in the area of information technology, and to a geographical diversification of centers of innovation — with new hubs especially in Asia. The ability of non-Western actors to increasingly incorporate civilian innovation into defense applications has led, among other things, to the perception of a growing erosion of conventional deterrence and defense capabilities in relation to rising powers and new actors of international security.

#### Loss of leadership on emerging tech causes nuclear transition wars in Taiwan and Eastern Europe.

Kroenig & Gopalaswamy 18, \*Associate Professor of Government and Foreign Service at Georgetown University and Deputy Director for Strategy in the Scowcroft Center for Strategy and Security at the Atlantic Council. \*\*Director of the South Asia Center at the Atlantic Council. He holds a PhD in mechanical engineering with a specialization in numerical acoustics from Trinity College, Dublin. (Matthew & Bharath, 11-12-2018, "Will disruptive technology cause nuclear war?", *Bulletin of the Atomic Scientists*, https://thebulletin.org/2018/11/will-disruptive-technology-cause-nuclear-war/)

Rather, we should think more broadly about how new technology might affect global politics, and, for this, it is helpful to turn to scholarly international relations theory. The dominant theory of the causes of war in the academy is the “bargaining model of war.” This theory identifies rapid shifts in the balance of power as a primary cause of conflict.

International politics often presents states with conflicts that they can settle through peaceful bargaining, but when bargaining breaks down, war results. Shifts in the balance of power are problematic because they undermine effective bargaining. After all, why agree to a deal today if your bargaining position will be stronger tomorrow? And, a clear understanding of the military balance of power can contribute to peace. (Why start a war you are likely to lose?) But shifts in the balance of power muddy understandings of which states have the advantage.

You may see where this is going. New technologies threaten to create potentially destabilizing shifts in the balance of power.

For decades, stability in Europe and Asia has been supported by US military power. In recent years, however, the balance of power in Asia has begun to shift, as China has increased its military capabilities. Already, Beijing has become more assertive in the region, claiming contested territory in the South China Sea. And the results of Russia’s military modernization have been on full display in its ongoing intervention in Ukraine.

Moreover, China may have the lead over the United States in emerging technologies that could be decisive for the future of military acquisitions and warfare, including 3D printing, hypersonic missiles, quantum computing, 5G wireless connectivity, and artificial intelligence (AI). And Russian President Vladimir Putin is building new unmanned vehicles while ominously declaring, “Whoever leads in AI will rule the world.”

If China or Russia are able to incorporate new technologies into their militaries before the United States, then this could lead to the kind of rapid shift in the balance of power that often causes war.

If Beijing believes emerging technologies provide it with a newfound, local military advantage over the United States, for example, it may be more willing than previously to initiate conflict over Taiwan. And if Putin thinks new tech has strengthened his hand, he may be more tempted to launch a Ukraine-style invasion of a NATO member.

Either scenario could bring these nuclear powers into direct conflict with the United States, and once nuclear armed states are at war, there is an inherent risk of nuclear conflict through limited nuclear war strategies, nuclear brinkmanship, or simple accident or inadvertent escalation.

This framing of the problem leads to a different set of policy implications. The concern is not simply technologies that threaten to undermine nuclear second-strike capabilities directly, but, rather, any technologies that can result in a meaningful shift in the broader balance of power. And the solution is not to preserve second-strike capabilities, but to preserve prevailing power balances more broadly.

#### US tech leadership prevents extinction from automation, strategic stability, genetic engineering

Jain 19 [Ash Jain is a senior fellow with the Scowcroft Center for Strategy and Security, where he oversees the Atlantic Council’s Democratic Order Initiative and D-10 Strategy Forum, Matthew Kroenig, "Present at the Re-Creation: A Global Strategy for Revitalizing, Adapting, and Defending a Rules-Based International System", 2019, https://www.atlanticcouncil.org/wp-content/uploads/2019/10/Present-at-the-Recreation.pdf]

The system must also be adapted to deal with new issues that were not envisioned when the existing order was designed. Foremost among these issues is emerging and disruptive technology, including AI, additive manufacturing (or 3D printing), quantum computing, genetic engineering, robotics, directed energy, the Internet of things (IOT), 5G, space, cyber, and many others. Like other disruptive technologies before them, these innovations promise great benefits, but also carry serious downside risks. For example, AI is already resulting in massive efficiencies and cost savings in the private sector. Routine tasks and other more complicated jobs, such as radiology, are already being automated. In the future, autonomous weapons systems may go to war against each other as human soldiers remain out of harm’s way.

Yet, AI is also transforming economies and societies, and generating new security challenges. Automation will lead to widespread unemployment. The final realization of driverless cars, for example, will put out of work millions of taxi, Uber, and long-haul truck drivers. Populist movements in the West have been driven by those disaffected by globalization and technology, and mass unemployment caused by automation will further grow those ranks and provide new fuel to grievance politics. Moreover, some fear that autonomous weapons systems will become “killer robots” that select and engage targets without human input, and could eventually turn on their creators, resulting in human extinction. The other technologies on this lisgt similarly balance great potential upside with great downside risk. 3D printing, for example, can be used to “make anything anywhere,” reducing costs for a wide range of manufactured goods and encouraging a return of local manufacturing industries.61 At the same time, advanced 3D printers can also be used by revisionist and rogue states to print component parts for advanced weapons systems or even WMD programs, spurring arms races and weapons proliferation.62 Genetic engineering can wipe out entire classes of disease through improved medicine, or wipe out entire classes of people through genetically engineered superbugs. Directed-energy missile defenses may defend against incoming missile attacks, while also undermining global strategic stability.

Perhaps the greatest risk to global strategic stability from new technology, however, comes from the risk that revisionist autocracies may win the new tech arms race. Throughout history, states that have dominated the commanding heights of technological progress have also dominated international relations. The United States has been the world’s innovation leader from Edison’s light bulb to nuclear weapons and the Internet. Accordingly, stability has been maintained in Europe and Asia for decades because the United States and its democratic allies possessed a favorable economic and military balance of power in those key regions. Many believe, however, that China may now have the lead in the new technologies of the twenty-first century, including AI, quantum, 5G, hypersonic missiles, and others. If China succeeds in mastering the technologies of the future before the democratic core, then this could lead to a drastic and rapid shift in the balance of power, upsetting global strategic stability, and the call for a democratic- led, rules-based system outlined in these pages.63

#### Licensing hikes and lack of legal clarity decimate AI innovation and threaten broader adoption

Ghafele 21 [Roya, visiting Professor in IP Law with the School of Law of Brunel University, Director of Oxfirst. “The Role of Standards and Patents in Artificial Intelligence”. 3/24/21. https://www.linkedin.com/pulse/role-standards-patents-artificial-intelligence-roya-ghafele?trk=public\_profile\_article\_view]

AI systems label a specific model of innovation that benefits from a wide range of contributors; be they inside or outside the firm. The role of patent law as an organizational principle of this type of ‘networked innovation’ remains yet to be adequately governed. In AI business thrives because of the interconnected framework in which it is embedded in.

The technological transformations enabled have triggered drastic modifications of the nature of economic exchange; making novel ways of doing business possible; not necessarily by owning devices protected by patents, but by owning access to a multitude of devices and facilitating easy interacting and exchange between them. Hence, the classical value proposition, whereby a single invention is protected through patent law and by consequence its owner has the right to exclude third parties from accessing it may risk to harm the nurturing eco system emerging from the standardization process.[1] In that regard, public policy formulation will need to play a major role, so to provide a governance structure that allows all players, be they large or small, to succeed. In particular it will require to study at greater length the role that patents that read on standards will and can play in this promising ecosystem.

This new economic context asks for a differentiated governance structure that assures in particular the functioning interplay between patents and standards. Against this background, this proposal suggests that the role of the FRAND (fair, reasonable and non-discriminatory) commitment should be further studied. Within a UK context in particular, it should be discussed to what extent it would not be appropriate to run another ‘Heargraves Review’ that addresses in greater detail the role of standard essential patents in the novel business environment provided by AI.

The Novel Economic Framework Provided by Artificial Intelligence

AI is still at its early stage and the opportunities it can offer have not even been seized yet to its full extent. At present, we do not even know the many different creative ways in which entrepreneurs will take AI forward. Entrepreneurs are experimenting with leveraging the AI in areas as vast as fashion or primary healthcare. Which businesses will ultimately prove viable remains still to be seen. AI is also big business. Investors expect growth rates as high as 20%.

In AI it is not the single device that creates value, but the ability to connect a sheer infinite number of devices with each other. The worth relies in the continuous expansion of the connection. It is the interconnectivity that creates value, not just the simple ownership of a single device.

At present most connected devices or telecom networks are controlled by humans. However, a key feature of the AI is that devices will be controlled by other devices (the controllers). These again can be classified in various ways, so to reflect the specific features of the controller. In the networked architecture of the AI various devices are at the same time receivers and suppliers of information; making it increasingly difficult to untangle the net of who provides and who receives proprietary technology and who adds value to the technology.

As such, Artificial Intelligence is a prototypical technology space, where Small and Medium Sized Enterprises (SMEs), universities and their spin-outs as well as big corporations alike could constitute a fruitful innovation ecosystem. All these players could thrive in the spirit of collaborative exchange, so to collectively re-invent the future of society, provided that adequate foundations are set for the role of patents within the context of AI.

The Need for Standards

Standard setting will be instrumental for the success of AI. It is only through a common language, the adoption of an interoperable and connected system that the wide spread use of AI can succeed. The process of standardisation will enhance innovation efficiency because it enhances compatibility and increases the credibility of technological solution. This standardisation process will likely be highly beneficial to the widespread dissemination of AI.

The success of a standard is based on its wide dissemination; its value derives from its vast usage. This stands in sharp contrast to patents, which are negative rights built around exclusivity. Contrary to a standard, the value of a patent derives from its strength to exclude to the best extent possible third parties from using it; unless obviously a third party is willing to pay for its usage.

This is why the inherent dilemma between patents and standards is hard to overcome. It is a tension between ‘free access and tight control.[2]’ This tensions is well pronounced in the standard essential patents debate. A patent declared essential to a standard is a strange hybrid that combines patent laws’ negative right’s aspect with a standard’s capability to disseminate a technology as wide as possible. As this formula bears the potential to accrue exceptional market power in the hands of patent owners, while at the same time rendering access to proprietary technology potentially very expensive, the (F)RAND (fair, reasonable and non- discriminatory) promise was introduced.

The (F)RAND rationale at its the core seeks to counter anti-competitive aspects of the licensing of standard essential patents. The (F)RAND commitment obligates SEPs owners to make their patents available on fair, reasonable and non-discriminatory terms. The reason why it does this, is because in the absence of doing so, there is a strong concern that opportunist behaviour can arise and by consequence competition in technology markets can be distorted.

Due to technical standard setting, there often arise only a handful of patent holders in a particular standard. This may be due to first mover advantages or because some firms have the necessary innovation capabilities to capture the patent landscape. It is alleged that these patent holders – having claimed an important position in the patent landscape – can charge abnormally high licensing rates to standard essential patent implementers; a phenomenon known as hold up.

Alongside those undesired consequences, royalty stacking can be another means to prevent downstream innovation. Royalty stacking can be defined as ‘situations in which a single product potentially infringes on many patents, and thus may bear multiple royalty burdens. The term 'royalty stacking' reflects the fact that, from the perspective of the firm making the product in question, all of the different claims for royalties must be added or 'stacked' together to determine the total royalty burden borne by the product if the firm is to sell that product free of patent litigation.’[3]

Research Questions

Nonetheless the (F)RAND commitment translates into an insufficiently complete contract between licensors and licensees. This is because of a built-in ambiguity over what “fair, reasonable and non-discriminatory” means; an ambiguity that is not addressed by means of the policies themselves but is expected to be resolved by “others”. This has led commentators such as Swanson & Baumol to argue that the (F)RAND commitment is of limited value in the absence of objective benchmarks that make clear the concrete terms or range of terms that are deemed to be reasonable and non- discriminatory.[4] This vagueness can lead to abuse and antitrust issues.[5] The situation is furthermore complicated by clandestine licensing markets and the absence of publicly available royalty rates that could be used as benchmarks to determine the value of a royalty rate of a SEPs.

Further issues pertain to a lack of clarity on ownership and distribution of patents that read on standards. Equally, there is lack of consistency as it pertains to the valuation of standard essential patents. Lack of clarity can also lead to a host of other unresolved challenges, such as negotiations taking potentially place in the shadow of the law and potential asymmetrical bargaining power between SEPs owners and downstream innovators.

#### AI innovation solves next gen cyberattacks

Dixon 19 [William, Head of Future Networks and Technology, World Economic Forum, Nicole Eagan, Chief Executive Officer, Darktrace. “3 ways AI will change the nature of cyber attacks”. 6/19/19. https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/]

Cyberattacks are becoming ubiquitous and have been recognized as one of the most strategically significant risks facing the world today. In recent years, we have witnessed digital assaults against governments and the owners of critical infrastructure, large private corporations and smaller ones, educational institutions and non-profit organizations. Not only is no sector immune from cyberattacks, the level of sophistication of the threats they face is continually increasing.

The future of cybersecurity will be driven by a new class of subtle and stealthy attackers that has recently emerged. Their aim is not to steal data, but rather to manipulate or change it. There is little doubt that artificial intelligence (AI) will be used by attackers to drive the next major upgrade in cyber weaponry and will ultimately pioneer the malicious use of AI. AI’s fundamental ability to learn and adapt will usher in a new era in which highly-customised and human-mimicking attacks are scalable. ’Offensive AI’ – highly sophisticated and malicious attack code – will be able to mutate itself as it learns about its environment, and to expertly compromise systems with minimal chance of detection.

Prototype-AI attacks: a glimpse into the future

AI-powered cyberattacks are not a hypothetical future concept. All the required building blocks for the use of offensive AI already exist: highly sophisticated malware, financially motivated – and ruthless – criminals willing to use any means possible to increase their return on investment, and open-source AI research projects which make highly valuable information available in the public domain.

One of the most notorious pieces of contemporary malware – the Emotet trojan – is a prime example of a prototype-AI attack. Emotet’s main distribution mechanism is spam-phishing, usually via invoice scams that trick users into clicking on malicious email attachments. The Emotet authors have recently added another module to their trojan, which steals email data from infected victims. The intention behind this email exfiltration capability was previously unclear, but Emotet has recently been observed sending out contextualized phishing emails at scale. This means it can automatically insert itself into pre-existing email threads, advising the victim to click on a malicious attachment, which then appears in the final, malicious email. This insertion of the malware into pre-existing emails gives the phishing email more context, thereby making it appear more legitimate.

Yet the criminals behind the creation of Emotet could easily leverage AI to supercharge this attack. Currently, the message on the final phishing email is usually highly generic - “Please see attached”, for instance - and this may sometimes arouse suspicion. However, by leveraging an AI’s ability to learn and replicate natural language by analysing the context of the email thread, these phishing emails could become highly tailored to individuals. This would mean that an AI-powered Emotet trojan could create and insert entirely customized, more believable phishing emails. Crucially, it would be able to send these out at scale, which would allow criminals to increase the yield of their operations enormously.

The consequences of these developing attack methods could be highly destructive, and even life-threatening. By undermining data integrity, these stealthy attacks cause trust in organizations to falter, and may even cause systemic failures to occur. Imagine an oil rig using faulty geo-prospection data to drill for oil in the wrong place, or a physician making a diagnosis using compromised medical records. As the AI arms race continues, we can only expect this circle of innovation to escalate.

Offensive AI: a paradigm shift in cyberattacks

In 2017, the WannaCry ransomware attack hit organizations in over 150 countries around the world, marking the beginning of a new era in cyberattack sophistication. Its success lay in its ability to move laterally through an organization in a matter of seconds while paralysing hard drives, and the incident went on to inspire multiple copycat attacks. This cycle of “innovation” will continue, and attackers have already moved on to cryptocurrency mining malware, which secretly steals processing power to mine for digital currencies such as bitcoin, and banking trojans, a type of malware that steals financial data while masquerading as a genuine application.

The use of adversarial artificial intelligence will impact the security landscape in three key ways:

1 - Impersonation of trusted users

AI attacks will be highly tailored yet operate at scale. These malwares will be able to learn the nuances of an individual’s behaviour and language by analysing email and social media communications. They will be able to use this knowledge to replicate a user’s writing style, crafting messages that appear highly credible. Messages written by AI malware will therefore be almost impossible to distinguish from genuine communications. As the majority of attacks get into our systems through our inboxes, even the most cyber-aware computer user will be vulnerable.

2 - Blending into the background

Sophisticated threat actors can often maintain a long-term presence in their target environments for months at a time, without being detected. They move slowly and with caution, to evade traditional security controls and are often targeted to specific individuals and organizations. AI will also be able to learn the dominant communication channels and the best ports and protocols to use to move around a system, discretely blending in with routine activity. This ability to disguise itself amid the noise will mean that it is able to expertly spread within a digital environment, and stealthily compromise more devices than ever before. AI malware will also be able to analyse vast volumes of data at machine speed, rapidly identifying which data sets are valuable and which are not. This will save the (human) attacker a great deal of time and effort.

3 - Faster attacks with more effective consequences

Today’s most sophisticated attacks require skilled technicians to conduct research on their target and identify individuals of interest, understand their social network and observe over time how they interact with digital platforms. In tomorrow’s world, an offensive AI will be able to achieve the same level of sophistication in a fraction of the time, and at many times the scale.

Not only will AI-driven attacks be much more tailored and consequently more effective, their ability to understand context means they will be even harder to detect. Traditional security controls will be impotent against this new threat, as they can only spot predictable, pre-modelled activity. AI is constantly evolving and will become ever-more resistant to the categorization of threats that remains fundamental to the modus operandi of legacy security approaches.

Incorporating AI in the digital ecosystem

As we increasingly rely on connected systems and devices, we are quickly developing a highly advanced and heavily connected digital ecosystem. We will require partnerships and capabilities that prioritize winning the strategic battles that count – and safeguard not only economically valuable data held by the public and private sectors, but the confidence in digital systems that underpins social cohesion and democratic institutions.

Investment in new technology will play a critical role in this emerging reality and evolving ecosystem. According to Forrester’s Using AI for Evil report, “mainstream AI-powered hacking is just a matter of time”. Indeed, as we begin to see AI become part of the cyber attacker’s toolkit, the only way that we will be able to combat this malicious use of AI is with AI itself. Therefore, incorporating the technology into this ecosystem is crucial.

Counterattack: Fighting machine with machine

The cybersecurity community is already heavily investing in this new future, and is using AI solutions to rapidly detect and contain any emerging cyberthreats that have the potential to disrupt or compromise key data. Defensive AI is not merely a technological advantage in fighting cyberattacks, but a vital ally on this new battlefield. Rather than rely on security personnel to respond to incidents manually, organizations will instead use AI to fight back against a developing problem in the short term, while human teams will oversee the AI’s decision-making and perform remedial work that improves overall resilience in the long term.

AI-powered attacks will outpace human response teams and outwit current legacy-based defenses; therefore, the mutually-dependent partnership of human and AI will be the bedrock of defense strategies in the future. The battleground of the future is digital, and AI is the undisputed weapon of choice. There is no silver bullet to the generational challenge of cybersecurity, but one thing is clear: only AI can play AI at its own game. The technology is available, and the time to prepare is now.

#### Competitive innovation prevents digital monocultures that create fatal critical infrastructure vulnerabilities.

Charles Duan 19, Director of Technology and Innovation Policy, R Street Institute, Washington, D.C., “Of Monopolies and Monocultures: The Intersection of Patents and National Security,” Santa Clara High Technology Law Journal, vol. 36, no. 4, 2020/2019, pp. 369–406

III. COMPETITION AND CYBERSECURITY

In addition to the historical review done so far, another approach to understanding the relationship among patents, competition, and national security is to consider the role of cybersecurity. There is little doubt that computer system vulnerabilities that enable hacking and spread of computer exploits are a threat to the nation's defenses, so better cybersecurity is a key part of national security strategy. 155 Strong competition can thus complement national security by enhancing domestic cybersecurity, and patent assertion that unduly weakens competition detracts from cybersecurity.5 6 Competition promotes better cybersecurity in at least two ways. First, multiple studies show that competition encourages firms to improve their products on multiple vectors including cybersecurity. Second, competition avoids a situation that security experts call a "monoculture," which increases vulnerability to severe cyberattacks. As former Secretary of Homeland Security Michael Chertoff wrote recently, "We need competition and multiple providers, not a potentially vulnerable technological monoculture," to guarantee national security. 5 7 Thus, cybersecurity provides a useful lens for understanding how unfettered patent assertion and licensing can detract from national security.

A. Cybersecurity as Competitive Value-Add

Competition enhances national security by reducing the incidence of technical vulnerabilities. That effect is especially important for security- sensitive systems such as mobile telecommunications.

Intuitively, a causal chain from competition to cybersecurity makes logical sense. Computer security is a value-added benefit to consumers, so firms in competitive markets are likely to use security to gain an edge over their competitors.158 In monopolized markets, though, there may be less external impetus to test products for flaws, and the monopolist may choose to focus less on security and more on new product features or increased product quality.

Economic research confirms these hypotheses about competition leading to better cybersecurity. A 2009 empirical study of web browsers considered the impact of market concentration on the amount of time that vendors took to fix security vulnerabilities as they were discovered. 9 The study found that the presence of more competitors correlated with faster cybersecurity response-a reduction of 8-10 days in response time per additional market rival.16 Similarly, business researchers in 2005 modeled incentives for firms to engage in sharing of cybersecurity information, and concluded that the "inclination to share information and invest in security technologies increases as the degree of competitiveness in an industry increases. ' 161 Another study found that, where two software firms are in competition, at least one will be willing to take on some degree of risk and responsibility for cybersecurity, whereas a monopoly software firm will consistently fail to accept such responsibility. 162 To be sure, an unpublished study from 2017 found that some market concentration can make firms more responsive to cybersecurity issues, but only to a point: "being in a dominant position reduces the positive effect of having less competitors on the responsiveness of the vendor," and indeed the "more dominant the firm is, the less rapid it is in releasing security patches."1 63 This research confirms that competition is more conducive to cybersecurity.

It is not hard to see how this applies to emerging communication technologies markets. In the absence of competition, the above research suggests that device manufacturers, chip makers, and software developers will lack incentives to respond to vulnerabilities, to share information about cybersecurity practices and issues, and to take responsibility for security matters. Mobile phone chips have had their share of cybersecurity failures already. 164 The best way to flush out ongoing and future cybersecurity issues is to maintain competitive pressure at all levels of the supply chain.

B. Vulnerabilities of "Monocultures"

A second reason why monopoly undermines cybersecurity is that monopoly leads to a "monoculture" of single-vendor products, opening the door to massive systemic failure in the case of a cyberattack. Computer researchers developed the theory of software monocultures in the early 2000s, in response to the regular phenomenon of computer viruses and other attacks spreading rapidly by exploiting flaws in the dominant operating system at the time, Microsoft Windows. 165 Where a computer system such as Windows has a commanding share of users, a virus that exploits a flaw in that system can quickly spread to infect a whole interconnected ecosystem. An operating system monopoly thus enables fast and easy spread of cyberattacks, and better cybersecurity would be achieved through greater diversity in online systems.166 As one research group posited, "a network architecture that supports a collection of heterogeneous network elements for the same functional capability offers a greater possibility of surviving security attacks as compared to homogeneous networks."1'67

There has been considerable study of the theory that computer monocultures are naturally more vulnerable to attacks.168 In one study, computer science researchers reviewed a catalog of 6,340 software vulnerabilities recorded in 2007, to compare whether comparable software would share the same flaws. 169 Of the 2,627 vulnerabilities applicable to application software (as opposed to operating systems, web scripts, and other software components), only 29 (1.1%) applied to substitute products from different vendors but providing the same functionality. 17 By contrast, different versions of a single software product were found to share vulnerabilities 84.7% of the time. 171 Thus, software monocultures share exploitable flaws even when there is some variation in versions across the monoculture; by contrast, diversity in software is almost guaranteed to prevent a single flaw from affecting all users.

In the case of 5G and wireless mobile communications, a monoculture is an especially concerning possibility. To the extent that systems such as smart city sensors or communication networks are widely deployed in a monoculture fashion, a widespread attack could have devastating consequences, potentially blacking out a region and affecting essential services such as 911.172 A monoculture that is vulnerable to so-called "rootkits" or "backdoors"-maliciously installed software that enable bad actors to commandeer systems-could also enable mass surveillance or spying by private hackers or foreign governments. 173 The presence of systems from multiple vendors would mitigate these possibilities.

The monoculture theory is not without critics, but a review of those criticisms shows them to be inapplicable to contemporary communication technologies. Some critics suggest that software diversity imposes unwarranted costs on firms who must forego economies of scale and devise seemingly duplicative yet different setups of computer systems. 174 But those concerns largely focus on the situation where a single firm produces and manages heterogeneous systems, concerns that are avoided where heterogeneity arises naturally through competition between two unrelated firms. Critics also argue that technological measures can create "artificial diversity" through automated randomization of software code, so software engineers can purportedly solve monoculture issues and device users need not worry about the issue. 175 But even these critics acknowledge that artificial diversity techniques are often insufficient because they must make assumptions about what aspects of the technology are most vulnerable to attack, and they concede that artificial diversity cannot stop attacks involving operation of legitimate software functions in undesirable ways (sending span emails or deleting document files, for example). 176

It is widely recognized that a monoculture is unavoidable in at least one respect: Most connected devices will need to conform to technical standards. 177 5G, for example, is a technical standard developed by a private industry consortium called 3GPP. 178 A flaw in any such standard would render all mobile devices implementing the standard vulnerable to an identical attack. 179 Avoiding these sorts of systemic flaws in standards requires rigorous development, analysis, and testing of the standard in the development process, which in turn requires ensuring that as many firms as possible, especially firms that share basic American values, are involved in the development of those standards.180 Thus, the necessary standardization of information and communication technologies is perhaps the most important reason why a competitive communication technology market is essential to cybersecurity and national security.

#### Cyber war goes nuclear

Erik Gartzke &Jon R. Lindsay 17. Gartzke is at the Department of Political Science, University of California, San Diego; Lindsay is at the Munk School of Global Affairs, University of Toronto. 03/01/2017. “Thermonuclear Cyberwar.” Journal of Cybersecurity, vol. 3, no. 1, pp. 37–48.

Cyber warfare is routinely overhyped as a new weapon of mass destruction, but when used in conjunction with actual weapons of mass destruction, severe, and underappreciated, dangers emerge. One side of a stylized debate about cybersecurity in international relations argues that offensive advantages in cyberspace empower weaker nations, terrorist cells, or even lone rogue operators to paralyze vital infrastructure [4–8]. The other side argues that operational difficulties and effective deterrence restrains the severity of cyber attack, while governments and cybersecurity firms have a pecuniary interest in exaggerating the threat [9–13]. Although we have contributed to the skeptical side of this debate [14–16], \*\*\*BEGIN FOOTNOTE\*\*\* 14. Gartzke E. The myth of cyberwar: bringing war in cyberspace back down to earth. Int Security 2013;38:41–73. Google ScholarCrossRef 15 Lindsay JR. Stuxnet and the limits of cyber warfare. Security Stud 2013;22:365–404. Google ScholarCrossRef 16 Lindsay JR. The impact of China on cybersecurity: fiction and friction. Int Security 2014;39:7–47. Google ScholarCrossRef \*\*\*END FOOTNOTE\*\*\* the same strategic logic that leads us to view cyberwar as a limited political instrument in most situations also leads us to view it as incredibly destabilizing in rare situations. In a recent Israeli wargame of a regional scenario involving the United States and Russia, one participant remarked on “how quickly localized cyber events can turn dangerously kinetic when leaders are ill-prepared to deal in the cyber domain” [17]. Importantly, this sort of catalytic instability arises not from the cyber domain itself but through its interaction with forces and characteristics in other domains (land, sea, air, etc.). Further, it arises only in situations where actors possess, and are willing to use, robust traditional military forces to defend their interests. Classical deterrence theory developed to explain nuclear deterrence with nuclear weapons, but different types of weapons or combinations of operations in different domains can have differential effects on deterrence and defense [18, 19]. Nuclear weapons and cyber operations are particularly complementary (i.e. nearly complete opposites) with respect to their strategic characteristics. Theorists and practitioners have stressed the unprecedented destructiveness of nuclear weapons in explaining how nuclear deterrence works, but it is equally, if not more, important for deterrence that capabilities and intentions are clearly communicated. As quickly became apparent, public displays of their nuclear arsenals improved deterrence.x At the same time, disclosing details of a nation’s nuclear capabilities did not much degrade the ability to strike or retaliate, given that defense against nuclear attack remains extremely difficult. Knowledge of nuclear capabilities is necessary to achieve a deterrent effect [20]. Cyber operations, in contrast, rely on undisclosed vulnerabilities, social engineering, and creative guile to generate indirect effects in the information systems that coordinate military, economic, and social behavior. Revelation enables crippling countermeasures, while the imperative to conceal capabilities constrains both the scope of cyber operations and their utility for coercive signaling [21, 22]. The diversity of cyber operations and confusion about their effects also contrast with the obvious destructiveness of nuclear weapons. The problem is that transparency and deception do not mix well. An attacker who hacks an adversary’s nuclear command and control apparatus, or the weapons themselves, will gain an advantage in warfighting that the attacker cannot reveal, while the adversary will continue to believe it wields a deterrent that may no longer exist. Most analyses of inadvertent escalation from cyber or conventional to nuclear war focus on “use it or lose it” pressures and fog of war created by attacks that become visible to the target [23, 24]. In a US–China conflict scenario, for example, conventional military strikes in conjunction with cyber attacks that blind sensors and confuse decision making could generate incentives for both sides to rush to preempt or escalate [25–27]. These are plausible concerns, but the revelation of information about a newly unfavorable balance of power might also cause hesitation and lead to compromise. Cyber blinding could potentially make traditional offensive operations more difficult, shifting the advantage to defenders and making conflict less likely. Clandestine attacks that remain invisible to the target potentially present a more insidious threat to crisis stability. There are empirical and theoretical reasons for taking seriously the effects of offensive cyber operations on nuclear deterrence, and we should expect the dangers to vary with the relative cyber capabilities of the actors in a crisis interaction. Nuclear command and control vulnerability General Robert Kehler, commander of US Strategic Command (STRATCOM) in 2013, stated in testimony before the Senate Armed Services Committee, “we are very concerned with the potential of a cyber-related attack on our nuclear command and control and on the weapons systems themselves” [28]. Nuclear command, control, and communications (NC3) form the nervous system of the nuclear enterprise spanning intelligence and early warning sensors located in orbit and on Earth, fixed and mobile command and control centers through which national leadership can order a launch, operational nuclear forces including strategic bombers, land-based intercontinental missiles (ICBMs), submarine-launched ballistic missiles (SLBMs), and the communication and transportation networks that tie the whole apparatus together [29, 30]. NC3 should ideally ensure that nuclear forces will always be available if authorized by the National Command Authority (to enhance deterrence) and never used without authorization (to enhance safety and reassurance). Friendly errors or enemy interference in NC3 can undermine the “always-never” criterion**,** weakening deterrence [31, 32]. NC3 has long been recognized as the weakest link in the US nuclear enterprise. According to a declassified official history, a Strategic Air Command (SAC) task group in 1979 “reported that tactical warning and communications systems … were ‘fragile’ and susceptible to electronic countermeasures, electromagnetic pulse, and sabotage, which could deny necessary warning and assessment to the National Command Authorities” [33]. Two years later, the Principal Deputy Under Secretary of Defense for Research and Engineering released a broad-based, multiservice report that doubled down on SAC’s findings: “the United States could not assure survivability, endurability, or connectivity of the national command authority function” due to: major command, control, and communications deficiencies: in tactical warning and attack assessment where existing systems were vulnerable to disruption and destruction from electromagnetic pulse, other high altitude nuclear effects, electronic warfare, sabotage, or physical attack; in decision making where there was inability to assure national command authority survival and connection with the nuclear forces, especially under surprise conditions; and in communications systems, which were susceptible to the same threats above and which could not guarantee availability of even minimum-essential capability during a protracted war. [33] The nuclear weapons safety literature likewise provides a number of troubling examples of NC3 glitches that illustrate some of the vulnerabilities attackers could, in principle, exploit [34–36]. The SAC history noted that NORAD has received numerous false launch indications from faulty computer components, loose circuits, and even a nuclear war training tape loaded by mistake into a live system that produced erroneous Soviet launch indications [33]. In a 1991 briefing to the STRATCOM commander, a Defense Intelligence Agency targeteer confessed, “Sir, I apologize, but we have found a problem with this target. There is a mistake in the computer code … . Sir, the error has been there for at least the life of this eighteen-month planning cycle. The nature of the error is such that the target would not have been struck” [37]. It would be a difficult operation to intentionally plant undetected errors like this, but the presence of bugs does reveal that such a hack is possible. Following many near-misses and self-audits during and after the Cold War, American NC3 improved with the addition of new safeguards and redundancies. As General Kehler pointed out in 2013, “the nuclear deterrent force was designed to operate through the most extreme circumstances we could possibly imagine” [28]. Yet vulnerabilities remain. In 2010, the US Air Force lost contact with 50 Minuteman III ICBMs for an hour because of a faulty hardware circuit at a launch control center [38]. If the accident had occurred during a crisis, or the component had been sabotaged, the USAF would have been unable to launch and unable to detect and cancel unauthorized launch attempts. As Bruce Blair, a former Minuteman missileer, points out, during a control center blackout the antennas at unmanned silos and the cables between them provide potential surreptitious access vectors [39]. The unclassified summary of a 2015 audit of US NC3 stated that “known capability gaps or deficiencies remain” [40]. Perhaps more worrisome are the unknown deficiencies. A 2013 Defense Science Board report on military cyber vulnerabilities found that while the: nuclear deterrent is regularly evaluated for reliability and readiness … , most of the systems have not been assessed (end-to-end) against a [sophisticated state] cyber attack to understand possible weak spots. A 2007 Air Force study addressed portions of this issue for the ICBM leg of the U.S. triad but was still not a complete assessment against a high-tier threat. [41] If NC3 vulnerabilities are unknown, it is also unknown whether an advanced cyber actor would be able to exploit them. As Kehler notes, “We don’t know what we don’t know” [28]. Even if NC3 of nuclear forces narrowly conceived is a hard target, cyber attacks on other critical infrastructure in preparation to or during a nuclear crisis could complicate or confuse government decision making. General Keith Alexander, Director of the NSA in the same Senate hearing with General Kehler, testified that: our infrastructure that we ride on, the power and the communications grid, are one of the things that is a source of concern … we can go to backup generators and we can have independent routes, but … our ability to communicate would be significantly reduced and it would complicate our governance … . I think what General Kehler has would be intact … [but] the cascading effect … in that kind of environment … concerns us. [28] Kehler further emphasized that “there’s a continuing need to make sure that we are protected against electromagnetic pulse and any kind of electromagnetic interference” [28]. Many NC3 components are antiquated and hard to upgrade, which is a mixed blessing. Kehler points out, “Much of the nuclear command and control system today is the legacy system that we’ve had. In some ways that helps us in terms of the cyber threat. In some cases it’s point to point, hard-wired, which makes it very difficult for an external cyber threat to emerge” [28]. The Government Accountability Office notes that the “Department of Defense uses 8-inch floppy disks in a legacy system that coordinates the operational functions of the nation’s nuclear forces” [42]. While this may limit some forms of remote access, it is also indicative of reliance on an earlier generation of software when security engineering standards were less mature. Upgrades to the digital Strategic Automated Command and Control System planned for 2017 have the potential to correct some problems, but these changes may also introduce new access vectors and vulnerabilities [43]. Admiral Cecil Haney, Kehler’s successor at STRATCOM, highlighted the challenges of NC3 modernization in 2015: Assured and reliable NC3 is fundamental to the credibility of our nuclear deterrent. The aging NC3 systems continue to meet their intended purpose, but risk to mission success is increasing as key elements of the system age. The unpredictable challenges posed by today’s complex security environment make it increasingly important to optimize our NC3 architecture while leveraging new technologies so that NC3 systems operate together as a core set of survivable and endurable capabilities that underpin a broader, national command and control system. [44] In no small irony, the internet itself owes its intellectual origin, in part, to the threat to NC3 from large-scale physical attack. A 1962 RAND report by Paul Baran considered “the problem of building digital communication networks using links with less than perfect reliability” to enable “stations surviving a physical attack and remaining in electrical connection … to operate together as a coherent entity after attack” [45]. Baran advocated as a solution decentralized packet switching protocols, not unlike those realized in the ARPANET program. The emergence of the internet was the result of many other factors that had nothing to do with managing nuclear operations, notably the meritocratic ideals of 1960s counterculture that contributed to the neglect of security in the internet’s founding architecture [46, 47]. Fears of NC3 vulnerability helped to create the internet, which then helped to create the present-day cybersecurity epidemic, which has come full circle to create new fears about NC3 vulnerability. NC3 vulnerability is not unique to the United States. The NC3 of other nuclear powers may even be easier to compromise, especially in the case of new entrants to the nuclear club like North Korea. Moreover, the United States has already demonstrated both the ability and willingness to infiltrate sensitive foreign nuclear infrastructure through operations such as Olympic Games (Stuxnet), albeit targeting Iran’s nuclear fuel cycle rather than NC3. It would be surprising to learn that the United States has failed to upgrade its Cold War NC3 attack plans to include offensive cyber operations against a wide variety of national targets. Hacking the deterrent The United States included NC3 attacks in its Cold War counterforce and damage limitation war plans, even as contemporary critics perceived these options to be destabilizing for deterrence [48]. The best known example of these activities and capabilities is a Special Access Program named Canopy Wing. East German intelligence obtained the highly classified plans from a US Army spy in Berlin, and the details began to emerge publicly after the Cold War. An East German intelligence officer, Markus Wolf, writes in his memoir that Canopy Wing “listed the types of electronic warfare that would be used to neutralize the Soviet Union and Warsaw Pact’s command centers in case of all-out war. It detailed the precise method of depriving the Soviet High Command of its high-frequency communications used to give orders to its armed forces” [49]. It is easy to see why NC3 is such an attractive target in the unlikely event of a nuclear war. If for whatever reason deterrence fails and the enemy decides to push the nuclear button, it would obviously be better to disable or destroy missiles before they launch than to rely on possibly futile efforts to shoot them down, or to accept the loss of millions of lives. American plans to disable Soviet NC3 with electronic warfare, furthermore, would have been intended to complement plans for decapitating strikes against Soviet nuclear forces. Temporary disabling of information networks in isolation would have failed to achieve any important strategic objective. A blinded adversary would eventually see again and would scramble to reconstitute its ability to launch its weapons, expecting that preemption was inevitable in any case. Reconstitution, moreover, would invalidate much of the intelligence and some of the tradecraft on which the blinding attack relied. Capabilities fielded through Canopy Wing were presumably intended to facilitate a preemptive military strike on Soviet NC3 to disable the ability to retaliate and limit the damage of any retaliatory force that survived, given credible indications that war was imminent. Canopy Wing included [50]: “Measures for short-circuiting … communications and weapons systems using, among other things, microscopic carbon-fiber particles and chemical weapons.” “Electronic blocking of communications immediately prior to an attack, thereby rendering a counterattack impossible.” “Deployment of various weapons systems for instantaneous destruction of command centers, including pin-point targeting with precision-guided weapons to destroy ‘hardened bunkers’.” “Use of deception measures, including the use of computer-simulated voices to override and substitute false commands from ground-control stations to aircraft and from regional command centers to the Soviet submarine fleet.” “Us[e of] the technical installations of ‘Radio Free Europe/Radio Liberty’ and ‘Voice of America,’ as well as the radio communications installations of the U.S. Armed Forces for creating interference and other electronic effects.” Wolf also ran a spy in the US Air Force who disclosed that the Americans had managed to penetrate the [Soviet air base at Eberswalde]’s ground-air communications and were working on a method of blocking orders before they reached the Russian pilots and substituting their own from West Berlin. Had this succeeded, the MiG pilots would have received commands from their American enemy. It sounded like science fiction, but, our experts concluded, it was in no way impossible that they could have pulled off such a trick, given the enormous spending and technical power of U.S. military air research. [49] One East German source claimed that Canopy Wing had a $14.5 billion budget for research and operational costs and a staff of 1570 people, while another claimed that it would take over 4 years and $65 million to develop “a prototype of a sophisticated electronic system for paralyzing Soviet radio traffic in the high-frequency range” [50]. Canopy Wing was not cheap, and even so, it was only a research and prototyping program. Operationalization of its capabilities and integration into NATO war plans would have been even more expensive. This is suggestive of the level of effort required to craft effective offensive cyber operations against NC3. Preparation comes to naught when a sensitive program is compromised. Canopy Wing was caught in what we describe below as the cyber commitment problem, the inability to disclose a warfighting capability for the sake of deterrence without losing it in the process. According to New York Times reporting on the counterintelligence investigation of the East German spy in the Army, Warrant Officer James Hall, “officials said that one program rendered useless cost hundreds of millions of dollars and was designed to exploit a Soviet communications vulnerability uncovered in the late 1970's” [51]. This program was probably Canopy Wing. Wolf writes, “Once we passed [Hall’s documents about Canopy Wing] on to the Soviets, they were able to install scrambling devices and other countermeasures” [49]. It is tempting to speculate that the Soviet deployment of a new NC3 system known as Signal-A to replace Signal-M (which was most likely the one targeted by Canopy Wing) was motivated in part by Hall’s betrayal [50]. Canopy Wing underscores the potential and limitations of NC3 subversion. Modern cyber methods can potentially perform many of the missions Canopy Wing addressed with electronic warfare and other means, but with even greater stealth and precision. Cyber operations might, in principle, compromise any part of the NC3 system (early warning, command centers, data transport, operational forces, etc.) by blinding sensors, injecting bogus commands or suppressing legitimate ones, monitoring or corrupting data transmissions, or interfering with the reliable launch and guidance of missiles. In practice, the operational feasibility of cyber attack against NC3 or any other target depends on the software and hardware configuration and organizational processes of the target, the intelligence and planning capacity of the attacker, and the ability and willingness to take advantage of the effects created by cyber attack [52, 53]. Cyber compromise of NC3 is technically plausible though operationally difficult, a point to which we return in a later section. To understand which threats are not only technically possible but also probable under some circumstance, we further need a political logic of cost and benefit [14]. In particular, how is it possible for a crisis to escalate to levels of destruction more costly than any conceivable political reward? Canopy Wing highlights some of the strategic dangers of NC3 exploitation. Warsaw Pact observers appear to have been deeply concerned that the program reflected an American willingness to undertake a surprise decapitation attack: they said that it “sent ice-cold shivers down our spines” [50]. The Soviets designed a system called Perimeter that, not unlike the Doomsday Device in Dr. Strangelove, was designed to detect a nuclear attack and retaliate automatically, even if cut off from Soviet high command, through an elaborate system of sensors, underground computers, and command missiles to transmit launch codes [54]. Both Canopy Wing and Perimeter show that the United States and the Soviet Union took nuclear warfighting seriously and were willing to develop secret advantages for such an event. By the same token, they were not able to reveal such capabilities to improve deterrence to avoid having to fight a nuclear war in the first place. Nuclear deterrence and credible communication Nuclear weapons have some salient political properties. They are singularly and obviously destructive. They kill in more, and more ghastly, ways than conventional munitions through electromagnetic radiation, blast, firestorms, radioactive fallout, and health effects that linger for years. Bombers, ICBMs, and SLBMs can project warheads globally without significantly mitigating their lethality, steeply attenuating the conventional loss-of-strength gradient [55]. Defense against nuclear attack is very difficult, even with modern ballistic missile defenses, given the speed of incoming warheads and use of decoys; multiple warheads and missile volleys further reduce the probability of perfect interception. If one cannot preemptively destroy all of an enemy’s missiles, then there is a nontrivial chance of getting hit by some of them. When one missed missile can incinerate millions of people, the notion of winning a nuclear war starts to seem meaningless for many politicians. As defense seemed increasingly impractical, early Cold War strategists championed the threat of assured retaliation as the chief mechanism for avoiding war [56–59]. Political actors have issued threats for millennia, but the advent of nuclear weapons brought deterrence as a strategy to center stage. The Cold War was an intense learning experience for both practitioners and students of international security, rewriting well-worn realities more than once [60–62]. A key conundrum was the practice of brinkmanship. Adversaries who could not compete by “winning” a nuclear war could still compete by manipulating the “risk” of nuclear annihilation, gambling that an opponent would have the good judgment to back down at some point short of the nuclear brink. Brinkmanship crises—conceptualized as games of Chicken where one cannot heighten tensions without increasing the hazard of the mutually undesired outcome—require that decision makers behave irrationally, or possibly that they act randomly, which is difficult to conceptualize in practical terms [63]. The chief concern in historical episodes of chicken, such as the Berlin Crisis and Cuban Missile Crisis, was not whether a certain level of harm was possible, but whether an adversary was resolved enough, possibly, to risk nuclear suicide. The logical inconsistency of the need for illogic to win led almost from the beginning of the nuclear era to elaborate deductive contortions [64–66]. Both mutually assured destruction (MAD) and successful brinksmanship depend on a less appreciated, but no less fundamental, feature of nuclear weapons: political transparency. Most elements of military power are weakened by disclosure [67]. Military plans are considerably less effective if shared with an enemy. Conventional weapons become less lethal as adversaries learn what different systems can and cannot do, where they are located, how they are operated, and how to devise countermeasures and array defenses to blunt or disarm an attack. In contrast, relatively little reduction in destruction follows from enemy knowledge of nuclear capabilities. For most of the nuclear era, no effective defense existed against a nuclear attack. Even today, with evolving ABM systems, one ICBM still might get through and annihilate the capital city. Nuclear forces are more robust to revelation than other weapons, enabling nuclear nations better to advertise the harm they can inflict. The need for transparency to achieve an effective deterrent is driven home by the satirical Cold War film, Dr. Strangelove: “the whole point of a Doomsday Machine is lost, if you keep it a secret! Why didn’t you tell the world, eh?” During the real Cold War, fortunately, Soviet leaders paraded their nuclear weapons through Red Square for the benefit of foreign military attaches and the international press corps. Satellites photographed missile, bomber, and submarine bases. While other aspects of military affairs on both sides of the Iron Curtain remained closely guarded secrets, the United States and the Soviet Union permitted observers to evaluate their nuclear capabilities. This is especially remarkable given the secrecy that pervaded Soviet society. The relative transparency of nuclear arsenals ensured that the superpowers could calculate risks and consequences within a first-order approximation, which led to a reduction in severe conflict and instability even as political competition in other arenas was fierce [61, 68]. Recent insights about the causes of war suggest that divergent expectations about the costs and consequences of war are necessary for contests to occur [69–73]. These insights are associated with rationalist theories, such as deterrence theory itself. Empirical studies and psychological critiques of the rationality assumption have helped to refine models and bring some circumspection into their application, but the formulation of sound strategy (if not the execution) still requires the articulation of some rational linkage between cause and effect [19, 62, 74]. Many supposedly nonrational factors, moreover, simply manifest as uncertainty in strategic interaction. Our focus here is on the effect of uncertainty and ignorance on the ability of states and other actors to bargain in lieu of fighting. Many wars are a product of what adversaries do not know or what they misperceive, whether as a result of bluffing, secrecy, or intrinsic uncertainty [75, 76]. If knowledge of capabilities or resolve is a prerequisite for deterrence, then one reason for deterrence failure is the inability or unwillingness to credibly communicate details of the genuine balance of power, threat, or interests. Fighting, conversely, can be understood as a costly process of discovery that informs adversaries of their actual relative strength and resolve. From this perspective, successful deterrence involves instilling in an adversary perceptions like those that result from fighting, but before fighting actually begins. Agreement about the balance of power can enable states to bargain (tacit or overt) effectively without needing to fight, forging compromises that each prefers to military confrontation or even to the bulk of possible risky brinkmanship crises. Despite other deficits, nuclear weapons have long been considered to be stabilizing with respect to rational incentives for war(the risk of nuclear accidents is another matter) [77]. If each side has a secure second strike—or even a minimal deterrent with some nonzero chance of launching a few missiles—then each side can expect to gain little and lose much by fighting a nuclear war. Whereas the costs of conventional war can be more mysterious because each side might decide to hold something back and meter out its punishment due to some internal constraint or a theory of graduated escalation, even a modest initial nuclear exchange is recognized to be extremely costly. As long as both sides understand this and understand (or believe) that the adversary understands this as well, then the relationship is stable. Countries engage nuclear powers with considerable deference, especially over issues of fundamental national or international importance. At the same time, nuclear weapons appear to be of limited value in prosecuting aggressive action, especially over issues of secondary or tertiary importance, or in response to aggression from others at lower levels of dispute intensity. Nuclear weapons are best used for signaling a willingness to run serious risks to protect or extort some issue that is considered of vital national interest. As mentioned previously, both superpowers in the Cold War considered the warfighting advantages of nuclear weapons quite apart from any deterrent effect, and the United States and Russia still do. High-altitude bursts for air defense, electromagnetic pulse for frying electronics, underwater detonations for anti-submarine warfare, hardened target penetration, area denial, and so on, have some battlefield utility. Transparency per se is less important than weapon effects for warfighting uses, and can even be deleterious for tactics that depend on stealth and mobility. Even a single tactical nuke, however, would inevitably be a political event. Survivability of the second strike deterrent can also militate against transparency, as in the case of the Soviet Perimeter system, as mobility, concealment, and deception can make it harder for an observer to track and count respective forces from space. Counterforce strategies, platform diversity and mobility, ballistic missile defense systems, and force employment doctrine can all make it more difficult for one or both sides in a crisis to know whether an attack is likely to succeed or fail. The resulting uncertainty affects not only estimates of relative capabilities but also the degree of confidence in retaliation. At the same time, there is reason to believe that platform diversity lowers the risk of nuclear or conventional contests, because increasing the number of types of delivery platforms heightens second strike survivability without increasing the lethality of an initial strike [78]. While transparency is not itself a requirement for nuclear use, stable deterrence benefits to the degree to which retaliation can be anticipated, as well as the likelihood that the consequences of a first strike are more costly than any benefit. Cyber operations, in contrast, are neither robust to revelation nor as obviously destructive. The cyber commitment problem Deterrence (and compellence) uses force or threats of force to “warn” an adversary about consequences if it takes or fails to take an action. In contrast, defense (and conquest) uses force to “win” a contest of strength and change the material distribution of power. Sometimes militaries can change the distribution of information and power at the same time. Military mobilization in a crisis signifies resolve and displays a credible warning, but it also makes it easier to attack or defend if the warning fails. Persistence in a battle of attrition not only bleeds an adversary but also reveals a willingness to pay a higher price for victory. More often, however, the informational requirements of winning and warning are in tension. Combat performance often hinges on well-kept secrets, feints, and diversions. Many military plans and capabilities degrade when revealed. National security involves trade-offs between the goals of preventing war, by advertising capabilities or interests, and improving fighting power should war break out, by concealing capabilities and surprising the enemy. The need to conceal details of the true balance of power to preserve battlefield effectiveness gives rise to the military commitment problem [79, 80]. Japan could not coerce the United States by revealing its plan to attack Pearl Harbor because the United States could not credibly promise to refrain from reorienting defenses and dispersing the Pacific Fleet. War resulted not just because of what opponents did not know but because of what they could not tell each other without paying a severe price in military advantage. The military benefits of surprise (winning) trumped the diplomatic benefits of coercion (warning). Cyber operations, whether for disruption and intelligence, are extremely constrained by the military commitment problem. Revelation of a cyber threat in advance that is specific enough to convince a target of the validity of the threat also provides enough information potentially to neutralize it. Stuxnet took years and hundreds of millions of dollars to develop but was patched within weeks of its discovery. The Snowden leaks negated a whole swath of tradecraft that the NSA took years to develop. States may use other forms of covert action, such as publicly disavowed lethal aid or aerial bombing (e.g. Nixon’s Cambodia campaign), to discretely signal their interests, but such cases can only work to the extent that revelation of operational details fails to disarm rebels or prevent airstrikes [81]. Cyber operations, especially against NC3, must be conducted in extreme secrecy as a condition of the efficacy of the attack. Cyber tradecraft relies on stealth, stratagem, and deception [21]. Operations tailored to compromise complex remote targets require extensive intelligence, planning and preparation, and testing to be effective. Actions that alert a target of an exploit allow the target to patch, reconfigure, or adopt countermeasures that invalidate the plan. As the Defense Science Board points out, competent network defenders: can also be expected to employ highly-trained system and network administrators, and this operational staff will be equipped with continuously improving network defensive tools and techniques (the same tools we advocate to improve our defenses). Should an adversary discover an implant, it is usually relatively simple to remove or disable. For this reason, offensive cyber will always be a fragile capability. [41] The world’s most advanced cyber powers, the United States, Russia, Israel, China, France, and the United Kingdom, are also nuclear states, while India, Pakistan, and North Korea also have cyber warfare programs. NC3 is likely to be an especially well defended part of their cyber infrastructures. NC3 is a hard target for offensive operations, which thus requires careful planning, detailed intelligence, and long lead-times to avoid compromise. Cyberspace is further ill-suited for signaling because cyber operations are complex, esoteric, and hard for commanders and policymakers to understand. Most targeted cyber operations have to be tailored for each unique target (a complex organization not simply a machine), quite unlike a general purpose munition tested on a range. Malware can fail in many ways and produce unintended side effects, as when the Stuxnet code was accidentally released to the public. The category of “cyber” includes tremendous diversity: irritant scams, hacktivist and propaganda operations, intelligence collection, critical infrastructure disruption, etc. Few intrusions create consequences that rise to the level of attacks such as Stuxnet or BlackEnergy, and even they pale beside the harm imposed by a small war. Vague threats are less credible because they are indistinguishable from casual bluffing. Ambiguity can be useful for concealing a lack of capability or resolve, allowing an actor to pool with more capable or resolved states and acquiring some deterrence success by association. But this works by discounting the costliness of the threat. Nuclear threats, for example, are usually somewhat veiled because one cannot credibly threaten nuclear suicide. The consistently ambiguous phrasing of US cyber declaratory policy (e.g. “we will respond to cyber-attacks in a manner and at a time and place of our choosing using appropriate instruments of U.S. power” [82]) seeks to operate across domains to mobilize credibility in one area to compensate for a lack of credibility elsewhere, specifically by leveraging the greater robustness to revelation of military capabilities other than cyber. This does not mean that cyberspace is categorically useless for signaling, just as nuclear weapons are not categorically useless for warfighting. Ransomware attacks work when the money extorted to unlock the compromised host is priced below the cost of an investigation or replacing the system. The United States probably gained some benefits in general deterrence (i.e. discouraging the emergence of challenges as opposed to immediate deterrence in response to a challenge) through the disclosure of Stuxnet and the Snowden leaks. Both revelations compromised tradecraft, but they also advertised that the NSA probably had more exploits and tradecraft where they came from. Some cyber operations may actually be hard to mitigate within tactically meaningful timelines (e.g. hardware implants installed in hard-to-reach locations). Such operations might be revealed to coerce concessions within the tactical window created by a given operation, if the attacker can coordinate the window with the application of coercion in other domains. As a general rule, however, the cyber domain on its own is better suited for winning than warning [83]. Cyber and nuclear weapons fall on extreme opposite sides of this spectrum. Dangerous complements Nuclear weapons have been used in anger twice—against the Japanese cities Hiroshima and Nagasaki—but cyberspace is abused daily. Considered separately, the nuclear domain is stable and the cyber domain is unstable. In combination, the results are ambiguous. The nuclear domain can bound the intensity of destruction that a cyber attacker is willing to inflict on an adversary. US declaratory policy states that unacceptable cyber attacks may prompt a military response; while nuclear weapons are not explicitly threatened, neither are they withheld. Nuclear threats have no credibility at the low end, where the bulk of cyber attacks occur. This produces a cross-domain version of the stability–instability paradox, where deterrence works at the high end but is not credible, and thus encourages provocation, at low intensities. Nuclear weapons, and military power generally, create an upper bound on cyber aggression to the degree that retaliation is anticipated and feared [22, 83, 84]. In the other direction, the unstable cyber domain can undermine the stability of nuclear deterrence. Most analysts who argue that the cyber–nuclear combination is a recipe for danger focus on the fog of crisis decision making [85–87]. Stephen Cimbala points out that today’s relatively smaller nuclear arsenals may perversely magnify the attractiveness of NC3 exploitation in a crisis: “Ironically, the downsizing of U.S. and post-Soviet Russian strategic nuclear arsenals since the end of the Cold War, while a positive development from the perspectives of nuclear arms control and nonproliferation, makes the concurrence of cyber and nuclear attack capabilities more alarming” [88]. Cimbala focuses mainly on the risks of misperception and miscalculation that emerge when a cyber attack muddies the transparent communication required for opponents to understand one another’s interests, redlines, and willingness to use force, and to ensure reliable control over subordinate commanders. Thus a nuclear actor “faced with a sudden burst of holes in its vital warning and response systems might, for example, press the preemption button instead of waiting to ride out the attack and then retaliate” [85]. The outcome of fog of decision scenarios such as these depend on how humans react to risk and uncertainty, which in turn depends on bounded rationality and organizational frameworks that might confuse rational decision making [89, 90]. These factors exacerbate a hard problem. Yet within a rationalist framework, cyber attacks that have already created their effects need not trigger an escalatory spiral. While being handed a fait accompli may trigger an aggressive reaction, it is also plausible that the target’s awareness that its NC3 has been compromised in some way would help to convey new information that the balance of power is not as favorable as previously thought. This in turn could encourage the target to accommodate, rather than escalate. While defects in rational decision making are a serious concern in any cyber–nuclear scenario, the situation becomes even more hazardous when there are rational incentives to escalate. Although “known unknowns” can create confusion, to paraphrase Donald Rumsfeld, the “unknown unknowns” are perhaps more dangerous. A successful clandestine penetration of NC3 can defeat the informational symmetry that stabilizes nuclear relationships. Nuclear weapons are useful for deterrence because they impose a degree of consensus about the distribution of power; each side knows the other can inflict prohibitive levels of damage, even if they may disagree about the precise extent of this damage. Cyber operations are attractive precisely because they can secretly revise the distribution of power. NC3 neutralization may be an expensive and rarified capability in the reach of only a few states with mature signals intelligence agencies, but it is much cheaper than nuclear attack. Yet the very usefulness of cyber operations for nuclear warfighting ensure that deterrence failure during brinksmanship crises is more likely. Nuclear states may initiate crises of risk and resolve to see who will back down first, which is not always clear in advance. Chicken appears viable, ironically, because each player understands that a nuclear war would be a disaster for all, and thus all can agree that someone can be expected swerve. Nuclear deterrence should ultimately make dealing with an adversary diplomatically more attractive than fighting, provided that fighting is costly—as would seem evident for the prospect of nuclear war—and assuming that bargains are available to states willing to accept compromise rather than annihilation. If, however, one side knows, but the other does not, that the attacker has disabled the target’s ability to perceive an impending military attack, or to react to one when it is underway, then they will not have a shared understanding of the probable outcome of war, even in broad terms. Consider a brinksmanship crisis between two nuclear states where only one has realized a successful penetration of the rival’s NC3. The cyber attacker knows that it has a military advantage, but it cannot reveal the advantage to the target, lest the advantage be lost. The target does not know that it is at a disadvantage, and it cannot be told by the attacker for the same reason. The attacker perceives an imbalance of power while the target perceives a balance. A dangerous competition in risk taking ensues. The first side knows that it does not need to back down. The second side feels confident that it can stand fast and raise the stakes far beyond what it would be willing to if it understood the true balance of power. Each side is willing to escalate to create more risk for the other side, making it more likely that one or the other will conclude that deterrence has failed and move into warfighting mode to attempt to limit the damage the other can inflict. The targeted nature and uncertain effects of offensive cyber operations put additional pressure on decision makers. An intrusion will probably disable only part of the enemy’s NC3 architecture, not all of it (which is not only operationally formidable to achieve but also more likely to be noticed by the target). Thus the target may retain control over some nuclear forces, or conventional forces. The target may be tempted to use some of them piecemeal to signal a willingness to escalate further, even though it cannot actually escalate because of the cyber operation. The cyber attacker knows that it has escalation dominance, but when even a minor demonstration by the target can cause great damage, it is tempting to preempt this move or others like it. This situation would be especially unstable if only second strike but not primary strike NC3 was incapacitated. Uncertainty in the efficacy of the clandestine penetration would discount the attacker’s confidence in its escalation dominance, with a range of possible outcomes. Enough uncertainty would discount the cyber attack to nothing, which would have a stabilizing effect by returning the crisis to the pure nuclear domain. A little bit of uncertainty about cyber effectiveness would heighten risk acceptance while also raising the incentives to preempt as an insurance measure. Adding allies into the mix introduces additional instability. An ally emboldened by its nuclear umbrella might run provocative risks that it would be much more reluctant to embrace if it was aware that the umbrella was actually full of holes. Conversely, if the clandestine advantage is held by the state extending the umbrella, allies could become unnerved by the willingness of their defender to run what appear to be outsize risks, oblivious of the reasons for the defender’s confidence, creating discord in the alliance and incentives for self-protective action, leading to greater uncertainty about alliance solidarity. The direction of influence between the cyber and nuclear realms depends to large degree on which domain is the main arena of action. Planning and conducting cyber operations will be bounded by the ability of aggressors to convince themselves that attacks will remain secret, and by the confidence of nuclear nations in their invulnerability. Fears of cross-domain escalation will tend to keep instability in cyberspace bounded. However, if a crisis has risen to the point where nuclear threats are being seriously considered or made, then NC3 exploitation will be destabilizing. Brinksmanship crises seem to have receded in frequency since the Cuban Missile Crisis but may be more likely than is generally believed. President Vladimir Putin of Russia has insinuated more than once in recent years that his government is willing to use tactical nuclear weapons if necessary to support his policies. Cyber power and nuclear stability Not all crises are the same. Indeed, their very idiosyncrasies create the uncertainties that make bargaining failure more likely [75]. So far our analysis would be at home in the Cold War, with the technological novelty of cyber operations. Yet not every state has the same cyber capabilities or vulnerabilities. Variation in cyber power relations across dyads should be expected to affect the strategic stability of nuclear states. The so-called second nuclear age differs from superpower rivalry in important ways [91]. There are fewer absolute numbers of warheads in the world, down from a peak of over 70 000 in the 1980s to about 15 000 today (less than 5000 deployed), but they are distributed very unevenly [92]. The United States and Russia have comparably sized arsenals, each with a fully diversified triad of delivery platforms, while North Korea only has a dozen or so bombs and no meaningful delivery system (for now). China, India, Pakistan, Britain, France, and Israel have modest arsenals in the range of several dozen to a couple hundred weapons, but they have very different doctrines, conventional force complements, domestic political institutions, and alliance relationships. The recent nuclear powers lack the hard-won experience and shared norms of the Cold War to guide them through crises, and even the United States and Russia have much to relearn. Cyber warfare capacity also varies considerably across contemporary nuclear nations. The United States, Russia, Israel, and Britain are in the top tier, able to run sophisticated, persistent, clandestine penetrations. China is a uniquely active cyber power with ambitious cyber warfare doctrine, but its operational focus is on economic espionage and political censorship, resulting in less refined tradecraft and more porous defenses for military purposes [16]. France, India, and Pakistan also have active cyber warfare programs, while North Korea is the least developed cyber nation, depending on China for its expertise [93]. It is beyond the scope of this article to assess crisis dyads in detail, and data on nuclear and cyber power for these countries are shrouded in secrecy. Here, as a way of summing up the arguments above, we offer a few conjectures about how stylized aspects of cyber power affect crisis stability through incentives and key aspects of decision making. We do not stress relative nuclear weapon capabilities on the admittedly strong (and contestable) assumption that nuclear transparency in the absence of cyber operations would render nuclear asymmetry irrelevant for crisis bargaining because both sides would agree about the terrible consequences of conflict [94]. We also omit domestic or psychological variables that affect relative power assessments, although these are obviously important. Even if neither India nor Pakistan have viable cyber–nuclear capabilities, brinksmanship between them is dangerous for many other reasons, notably compressed decision timelines, Pakistan’s willingness to shoot first, and domestic regime instability. Our focus is on the impact of offensive and defensive cyber power on nuclear deterrence above and beyond the other factors that certainly play a role in real-world outcomes. First, does the cyber attacker have the organizational capacity, technical expertise, and intelligence support to “compromise” the target’s NC3? Can hackers access critical networks, exploit technical vulnerabilities, and confidently execute a payload to disrupt or exploit strategic sensing, command, forces, or transport capacity? The result would be some tangible advantage for warfighting, such as tactical warning or control paralysis, but one that cannot be exercised in bargaining. Second, is the target able to “detect” the compromise of its NC3? The more complicated and sensitive the target, the more likely cyber attackers are to make a mistake that undermines the intrusion. Attribution is not likely to be difficult given the constricted pool of potential attackers, but at the same time the consequences of misattributing “false flag” operations could be severe [95]. At a minimum, detection is assumed to provide information to the target that the balance of power is perhaps not as favorable as imagined previously. We assume that detection without an actual compromise is possible because of false positives or deceptive information operations designed to create pessimism or paranoia. Third, is the target able to “mitigate” the compromise it detects? Revelation can prompt patching or network reconfiguration to block an attack, but this assumption is not always realistic. The attacker may have multiple pathways open or may have implanted malware that is difficult to remove in tactically meaningful timelines. In such cases the cyber commitment problem is not absolute, since the discovery of the power to hurt does not automatically disarm it. Successful mitigation here is assumed to restore mutual assessments of the balance of power to what they would be absent the cyber attack. Table 1 shows how these factors combine to produce different deterrence outcomes in a brinksmanship (chicken) crisis. If there is no cyber compromise and the target detects nothing (no false positives) then we have the optimistic ideal case where nuclear transparency affords stable “deterrence.” Transparency about the nuclear balance, including the viability of secure second strike forces, provides strategic stability. We also expect this box to describe situations where the target has excellent network defense capabilities and thus the prospect of defense, denial or deception successfully deters any attempts to penetrate NC3. This may resemble the Cold War situation (with electronic warfare in lieu of cyber), or even the present day US–Russia dyad, where the odds of either side pulling off a successful compromise against a highly capable defender are not favorable. Alternately the attack may be deemed risky enough to encourage serious circumspection. However, the existence of Canopy Wing does not encourage optimism in this regard. [[TABLE 1 OMITTED]] Conversely, if there is a compromise that goes undetected, then there is a heightened risk of “war” because of the cyber commitment problem. This box may be particularly relevant for asymmetric dyads such as the United States and North Korea, where one side has real cyber power but the other side is willing to go to the brink where it believes, falsely, that it has the capability to compel its counterpart to back down. Cyber disruption of NC3 is attractive for damage limitation should deterrence fail, given that the weaker state’s diminutive arsenal makes damage limitation by the stronger state more likely to succeed. The dilemma for the stronger state is that the clandestine counterforce hedge, which makes warfighting success more likely, is precisely what makes deterrence more likely to fail. The United States would face similar counterforce dilemmas with other dyads like China or even Russia, although even a strong cyber power should be more circumspect when confronted with an adversary with a larger/more capable nuclear and conventional arsenal. More complex and cyber savvy targets, moreover, are more likely to detect a breach in NC3, leading to more ambiguous outcomes depending on how actors cope with risk and uncertainty. Paradoxically, confidence in cyber security may be a major contributor to failure; believing one is safe from attack increases the chance that an attack is successful. If the successful compromise is detected but not mitigated, then the target learns that the balance of power is not as favorable as thought. This possibility suggests fleeting opportunities for “coercion” by revealing the cyber coup to the target in the midst of a crisis while the cyber attacker maintains or develops a favorable military advantage before the target has the opportunity to reverse or compensate the NC3 disruption. Recognizing the newly transparent costs of war, a risk neutral or risk averse target should prefer compromise. The coercive advantages (deterrence or compellence) of a detected but unmitigated NC3 compromise will likely be fleeting. This suggests a logical possibility for creating a window of opportunity for using particular cyber operations that are more robust to revelation as a credible signal of superior capability in the midst of a crisis. It would be important to exploit this fleeting advantage via other credible military threats (e.g. forces mobilized on visible alert or deployed into the crisis area) before the window closes. One side may be able gain an unearned advantage, an opportunity for coercion via a “bluff,” by the same window-of-opportunity logic. A target concerned about NC3 compromise will probably have some network monitoring system and other protections in place. Defensive systems can produce false positives as a result of internal errors or a deception operation by the attacker to encourage paranoia. It is logically possible that some false positives would appear to the target to be difficult to mitigate. In this situation, the target could believe it is at a disadvantage, even though this is not in fact the case. This gambit would be operationally very difficult to pull off with any reliability in a real nuclear crisis. Cyber–nuclear coercion and bluffing strategies are fraught with danger. Detection without mitigation might put a risk-acceptant or loss-averse target into a “use-lose” situation, creating pressures to preempt or escalate. The muddling of decision-making heightens the risk of accidents or irrational choices in a crisis scenario. Worry about preemption or accident then heightens the likelihood that the initiator will exercise counterforce options while they remain available. These pressures can be expected to be particularly intense if the target’s detection is only partial or has not revealed the true extent of damage to its NC3 (i.e. the target does not realize it has already lost some or all of what it hopes to use). These types of scenarios are most usually invoked in analyses of inadvertent escalation [23–27]. The essential distinction between “use-lose” risks and “war” in this typology is the target’s knowledge of some degree of NC3 compromise. Use-lose and other cognitive pressures can certainly result in nuclear war, since the breakdown of deterrence leads to the release of nuclear weapons, but we distinguish these outcomes to highlight the different decision making processes or rational incentives at work. A “spiral” of mistrust may emerge if one side attempts a compromise but the defender detects and mitigates it. Both sides again have common mutual estimates of the relative balance of power, which superficially resembles the “deterrence” case because the NC3 compromise is negated. Unfortunately, the detection of the compromise will provide the target with information about the hostile intentions of the cyber attacker. This in turn is likely to exacerbate other political or psychological factors in the crisis itself or in the crisis-proneness of the broader relationship. The strange logical case where there is no compromise but one is detected and mitigated could result from a false positive misperception (including a third-party false flag operation) that could conflict spiraling [96, 97]. The bluff and coercion outcomes are also likely to encourage spiraling behavior once the fleeting bargaining advantage dissipates or is dispelled (provided anyone survives the interaction). The risk of crisis instability is not the same for all dyads. It is harder to compromise the NC3 of strong states because of the redundancy and active defenses in their arsenal. Likewise, strong states are better able to compromise the NC3 of any states but especially of weaker states, because of strong states’ greater organizational capacity and expertise in cyber operations. Stable deterrence or MAD is most likely to hold in mutually strong dyads (e.g. the United States and the Soviet Union in the Cold War or Russia today to a lesser extent). Deterrence is slightly less likely in other equally matched dyads (India–Pakistan) where defensive vulnerabilities create temptations but offensive capabilities may not be sufficient to exploit them. Most states can be expected to refrain from targeting American NC3 given a US reputation for cyber power (a general deterrence benefit enhanced by Stuxnet and Snowden). The situation is less stable if the United States is the attacker. The most dangerous dyad is a stronger and a weaker state (United States and North Korea or Israel and Iran). Dyads involving strong and middle powers are also dangerous (United States and China**).** The stronger side is tempted to disrupt NC3 as a warfighting hedge in case deterrence breaks down, while the weaker but still formidable side has a reasonable chance at detection. The marginally weaker may also be tempted to subvert NC3, particularly for reconnaissance; the stronger side is more likely to detect and correct the intrusion but will be alarmed by the ambiguity in distinguishing intelligence collection from attack planning [98]. In a brinksmanship crisis between them, windows for coercion may be available yet fleeting, with real risks of spiral and war**.**

#### Actors have the means and motivations to strike critical infrastructure.

Wintch 21, \*Timothy M. Wintch, an active-duty Major in the United States Air Force. He is currently a graduate student at the Oettinger School of Science & Technology Intelligence, National Intelligence University, in Bethesda, Maryland. Mr. Wintch has over 11 years of experience in command-and-control operations as an Air Battle Manager. He holds a Bachelor of Arts in Politics from the University of California, Santa Cruz, and a Master of Arts in Military Studies from American Military University. (April 20th, 2021, “PERSPECTIVE: Cyber and Physical Threats to the U.S. Power Grid and Keeping the Lights on”, https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/)

Among critical infrastructure sectors in the U.S., energy is perhaps the most crucial of the 16 sectors defined by the Department of Homeland Security. This sector is so vital because it provides the energy necessary to run every other critical infrastructure sector. However, the U.S. power grid, the backbone of the energy sector, is built upon an aging skeleton that is becoming increasingly vulnerable every day. Whether from terrorists or nation-states like Russia and China, the power grid is susceptible to not just physical attacks, but also to cyber intrusion as well. However, much of this threat can be mitigated if the U.S. takes the appropriate steps to safeguard the power grid and avoid a potential catastrophe in the future.

Since Sept. 11, 2001, terrorism on U.S. soil has been at the forefront of American consciousness. Critical infrastructure provides an appealing target because of the disproportionally large impact even a small attack can have on the sectors. In particular, the power grid represents a particularly lucrative target, both in terms of the ease of access and the large impact it can make. The National Research Council stated that the U.S. power grid is “vulnerable to intelligent multi-site attacks by knowledgeable attackers intent on causing maximum physical damage to key components on a wide geographical scale.”[[1]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn1) Additionally, the physical security of transmission and distribution systems is difficult due to the dispersed nature of these key components, which in turn is advantageous to attackers as it reduces the likelihood of their capture.[[2]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn2) From 2002-2012, approximately 2,500 physical attacks occurred against transmission lines and towers worldwide and approximately 500 attacks against transformer substations.[[3]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn3) Terrorists have the motivation to attack the U.S. power grid but the very nature of the grid makes it highly vulnerable. The power grid is not only at risk from physical attacks, but also nation-state cyberattacks.

One nation that has shown both the capability and intent to use attacks against critical energy infrastructure is Russia, as demonstrated in their 2015 annexation of Crimea from Ukraine. A Russian cyber threat group known as Sandworm, which used its BlackEnergy malware, attacked Ukrainian computer systems that provide remote control of the Ukraine power grid.[[4]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn4) This attack, and another in 2016, each left the capital Kiev without power, prompting cyber experts to raise concern about the same malware already existing in NATO and the U.S. power grids.[[5]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn5) In any conflict between Russia and NATO, not only would similar cyberattacks pose a threat, but so would potential physical attacks severing fuel oil and natural gas lines to Western Europe. Russia has both the capability and intent to attack critical infrastructure, particularly power grids, during future conflicts in their “hybrid warfare” approach.

Another nation that has the capability to attack critical energy infrastructure is China, representing a threat to not just the U.S. energy infrastructure but also that of our allies whose support would be vital in a major conflict. A recent NATO report highlighted this threat from China’s Belt and Road Initiative, stating that “[China’s] foreign direct investment in strategic sectors [such as energy generation and distribution] …raises questions about whether access and control over such infrastructure can be maintained, particularly in crisis when it would be required to support the military.”[[6]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn6) Like Russia, China has been active with cyber intrusions in U.S. energy infrastructure. The Mission Support Center at Idaho National Laboratory characterized these as attacks as “multiple intrusions into US ICS/SCADA [Industrial Control Systems/Supervisory Control and Data Acquisition] and smart grid tools [that] may be aimed more at intellectual property theft and gathering intelligence to bolster their own infrastructure, but it is likely that they are also using these intrusions to develop capabilities to attack the [bulk electric system], as well.”[[7]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn7) China, therefore, has both the capability and intent to conduct cyber intrusions and attacks for myriad reasons.

Another arm of this threat is the reliance the U.S. energy industry has on imports from China, especially transformers. In early 2020, federal officials seized a transformer in the port of Houston that had been imported by the Jiangsu Huapeng Transformer Company before sending it to Sandia National Laboratory in Albuquerque. Sandia is contracted by the U.S. Department of Energy for mitigating national security threats.[[8]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn8) The Wall Street Journal reported that “Mike Howard, chief executive of the Electric Power Research Institute, a utility-funded technical organization, said that the diversion of a huge, expensive transformer is so unusual – in his experience, unprecedented – that it suggests officials had significant security concerns.”[[9]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/" \l "_ftn9) Previously destined for the Washington Area Power Administration’s Ault, Colo., substation, the transformer is believed to have been seized due to “backdoor” exploitable hardware emplaced by the Chinese prior to shipment.[[10]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/#_ftn10) Shortly after these events, President Trump issued Executive Order 13920, “[Securing the United States Bulk-Power System](https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/),” essentially limiting the import of Chinese-built critical energy infrastructure components due to concerns about cybersecurity.[[11]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/#_ftn11) Interestingly, Jiangsu Huapeng “boasted that it supported 10 percent of New York City’s electricity load.”[[12]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/#_ftn12)

Franklin Kramer, the former Assistant Secretary of Defense for International Security Affairs, testified before a U.S. House of Representatives Energy and Commerce subcommittee during an energy and power hearing in 2011 and said that a “highly-coordinated and structured cyber, physical, or blended attack on the bulk power system, however, could result in long-term (irreparable) damage to key system components in multiple simultaneous or near-simultaneous strikes.” He added that “an outage could result with the potential to affect a wide geographic area and cause large population centers to lose power for extended periods.”[[13]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/#_ftn13) Even the inclusion of features such as smart grids to the overall grid structure poses new vulnerabilities through their connectivity. Kramer stated that “such connectivity means that the distribution system could be a key vector for a national security attack on the grid.”[[14]](https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/#_ftn14)

#### IoT innovation will be gutted by patent holdup – antitrust solves

Morton 16 [Fiona Scott Morton, Theodore Nierenberg Professor at Yale School of Management. Carl Shapiro, Former Director of the Institute of Business and Economic Research at UC Berkeley, Professor of the Graduate School at the Haas School of Business and the Department of Economics at the University of California at Berkeley. “Patent Assertions: Are We Any Closer to Aligning Reward to Contribution?”. 2016. https://www.journals.uchicago.edu/doi/full/10.1086/684987#\_i22]

However, our overall conclusions regarding SEPs are more mixed. Policy and legal changes that have reduced the ability of SEP owners to engage in patent holdup appear to have stalled out, especially as regards reform of the IPR rules at SSOs other than the IEEE. If so, this could have important effects on innovation and efficiency. For example, the “Internet of Things” is a new and growing area where royalty stacking and patent holdup appear to be very real dangers. Devices of all sorts, from thermostats to railroad cars to refrigerators, are being given connectivity using standards developed by SSOs. The price of those chips, and whether the IP contained in them costs $5 or $0.50 or $0.005, will determine the nature of new applications and the rate of adoption.

Failure to prevent patent holdup relating to tomorrow’s information technology and communications standards is likely to cause significant social welfare loss in the years ahead. If new and more effective private solutions relating to standard setting do not emerge to promote innovation and protect consumers, antitrust enforcement is one of the only remaining remedies that seems feasible.

V. Conclusions

Over the past five years, the rewards provided to patent owners in the United States have become more closely matched with the value of the technology they contribute. When rewards and contributions are aligned, economic efficiency is promoted because investments into developing new technologies are commensurate with benefits. These changes have come from legislation, the federal courts, and policy statements and enforcement actions by regulators of various types. However, at this juncture, we see a substantial gap persisting between the ability of some patent owners to monetize their patents and the contributions provided by the technology underlying those patents. With the “Internet of Things” poised to create economic growth, this is a problem worthy of further research and policy attention.

#### Solves extinction through resource efficiency

Maheswaran 20 [Mohan, Forbes Council Member on Forbes Technology Council. “Why The IoT Will Save Our Natural Resources”. https://www.forbes.com/sites/forbestechcouncil/2020/02/21/why-the-iot-will-save-our-natural-resources/?sh=49a24ad51be5]

Since the 18th century, industrialization and overconsumption have contributed to the rapid depletion of nature's raw materials. Smart connectivity carves a path for us to be more efficient in our use of these materials, effectively reducing the rate at which we are consuming and wasting natural resources.

According to the United Nations' Global Resources Outlook 2019 report, the worldwide use of natural resources has more than tripled in almost 50 years, with nonmetallic minerals witnessing a fivefold increase and fossil fuel use increasing over 45% over the same time frame.

To ensure that future generations have access to these resources and for the long-term survival of our planet, we must focus our efforts on managing the use of resources like water, gas and coal.

The emerging role of the IoT.

There are many IoT options for preserving natural resources, from tracking the bee population to reducing global carbon remissions, but implementing solutions into existing infrastructure can require a high investment in terms of resources like time and money.

IoT solutions with key capabilities such as long range and low power are more reliable and effective in enabling smart cities, smart enterprises and smart homes to manage resources more efficiently. Their emergence is enabling villages, cities and countries to rapidly and cost-effectively plan and transform themselves into smart communities that prepare a long-term vision for their people and their associated resources.

Long-range, low-power devices also remove the obstacle of capturing incorrect data and/or inaccurate analytics, as these devices provide data in real time that can assist with decision-making processes that help to conserve both exhaustible and inexhaustible resources. Such decisions might include the shutting down of pipelines due to leaks, the monitoring of excess resource use or simply the alert of a potential loss of valuable resources due to imperfect environmental conditions.

For example, according to a survey conducted by the Energy Information Administration, a large commercial building in the U.S. uses an average of at least 20,000 gallons of water per day, while statistics published by the Environmental Protection Agency show that each American uses approximately 88 gallons of water per day. The concern of water shortage is rising so much that in 2014, the Government Accountability Office noted that 40 out of 50 U.S. states expected water shortages over the next 10 years.

Smart water management systems can provide commercial buildings with status updates on how much water is used by the minute and can help predict where water issues could occur while providing valuable, timely information. For corporations with multiple locations, this approach to managing water can help save millions of gallons of water annually, as well as millions of dollars in overhead operation costs.

Embedding the IoT into the land, sea and sky.

Companies like Costco as well as cities across the world are deploying LoRa-enabled sensors to help preserve raw materials and natural resources. High water usage is a common concern among farmers. To maximize the growth of crop yields and to reduce water usage, some farmers are installing LoRa-based sensors to monitor water in real time.

Sensoterra, a technology company offering low-cost wireless solutions for real-time soil moisture measurement for commercial farms, partnered with my company to integrate LoRa-based sensors in its agriculture systems to reduce up to 30% of water usage in commercial farms, including potato and almond orchards. Reducing water usage on commercial farms helps conserve limited water supplies while allowing the farmers to focus more on their businesses.

Additionally, city and park authorities use movement sensors on bridges, roads and buildings to get real-time alerts in case of an impending natural disaster such as an earthquake. Another of our customers, handheld device company Beartooth, uses IoT sensors and enables users to talk, text and locate friends in a cellular network outage without the need for Wi-Fi, and the LoRa-based device has low power consumption.

Air pollution also poses a major risk to our environment and health. According to the World Health Organization, exposure to outdoor air pollution causes 4.2 million deaths per year. IoT sensors are able to collect air quality data to determine the areas causing dangerous air pollution in cities and facilitate the analytical management of suitable air quality control programs. Consumers and businesses have already realized the significance of collecting data and synthesizing it into meaningful patterns of information.

I believe the transition to intelligent information systems will be crucial as global environmental challenges accelerate. Deploying IoT solutions with LoRa-based sensors, together with edge network analytics, makes it possible to install intelligent sensor systems without requiring labor-intensive sensor battery replacements.

In general, deploying an IoT solution is usually complex. Currently, there are limited end-to-end solutions that are available as "out-of-the-box" solutions. Systems integrators are the proper companies to turn to for providing such end-to-end solutions and making sure the relevant back-end IT systems are integrated such that existing processes will benefit from the new IoT data captured from sensors.

One challenge for companies who would like to implement LoRaWAN is that not all countries have public LoRaWAN network providers with nationwide coverage. Some companies prefer to deploy applications that can connect to a broad public, nationwide coverage. However, users are also able to use a private LoRaWAN network, and some customers actually prefer to use a private network. Customers are able to manage the private network by themselves or have third parties like systems integrators manage the network. Such private networks even have benefits compared to public networks when it comes to flexibly deploying LoRa gateways wherever coverage is needed, whether it's indoors or outdoors.

The proliferation of long-range, ultra-low-power IoT sensors and networks is potentially the most important technology innovation in generations that will play a huge role in the buildout of smart cities that will help preserve our future natural resources.

#### Resource wars are the most likely cause of global conflict – scarcity is a conflict multiplier

Lehane 17 [Sinéad Lehane is research manager for Future Directions International’s Global Food and Water Crises Research program. Her current research projects include Australia’s food system and water security in the Tibetan Plateau region. Shaping Conflict in the 21st Century—The Future of Food and Water Security. February 2, 2017. www.hidropolitikakademi.org/shaping-conflict-in-the-21st-century-the-future-of-food-and-water-security.html]

In his book, The Coming Famine, Julian Cribb writes that the wars of the 21st century will involve failed states, rebellions, civil conflict, insurgencies and terrorism. All of these elements will be triggered by competition over dwindling resources, rather than global conflicts with clearly defined sides. More than 40 countries experienced civil unrest following the food price crisis in 2008. The rapid increase in grain prices and prevailing food insecurity in many states is linked to the outbreak of protests, food riots and the breakdown of governance. Widespread food insecurity is a driving factor in creating a disaffected population ripe for rebellion. Given the interconnectivity of food security and political stability, it is likely food will continue to act as a political stressor on regimes in the Middle East and elsewhere. Addressing Insecurity Improving food and water security and encouraging resource sharing is critical to creating a stable and secure global environment. While food and water shortages contribute to a rising cycle of violence, improving food and water security outcomes can trigger the opposite and reduce the potential for conflict. With the global population expected to reach 9 billion by 2040, the likelihood of conflict exacerbated by scarcity over the next century is growing. Conflict is likely to be driven by a number of factors and difficult to address through diplomacy or military force. Population pressures, changing weather, urbanization, migration, a loss of arable land and freshwater resources are just some of the multi-layered stressors present in many states. Future inter-state conflict will move further away from the traditional, clear lines of military conflict and more towards economic control and influence.

### 2

#### Solvency

#### The United States federal government should substantially increase antitrust prohibitions on standard essential patent holders that engage in anticompetitive licensing practices.

#### Applying antitrust to FRAND violations including refusals to deal solves collapsed innovation and market competition

Greene 19 [Kyle, J.D. Candidate Columbia Law. Columbia Business Law Review Writer and Honors intern @SEC. “Standard Essential Patents and Antitrust Law”. November 2019. https://journals.library.columbia.edu/index.php/CBLR/article/view/5120/2370]

III.ANTITRUST LIABILITY: WHEN SEP HOLDERS REFUSE TO DEAL

A.Reasons for a Presumption of Antitrust Liability

The affirmative case for a presumption of antitrust liability when a SEP holder refuses to deal with a prospective standard implementer in violation of its FRAND commitments proceeds, from the above discussion, as follows: (1) the standard setting process is of vital importance for many industries and technologies, but confers incredible and abusable power to SEP holders,141(2) despite Trinko, the Supreme Court has not ruled out either the essential facilities doctrine or an intent-based inquiry for a Sherman Act Section 2 refusal to deal case,142and (3) the leading circuit court decisions that consider refusals to deal by patent holders in general do not offer policy or legal objections which support an argument against presuming antitrust liability when the patent holder owns a standard essential patent.143As a result, a refusal to deal by an SEP holder is dangerously anticompetitive conduct that is—on its face—exactly the sort of conduct which has been, and should be, condemned by the antitrust laws.

Standards are crucial to the modern economy. But the factors that make standards valuable, even necessary, in so many industries are the same factors that lead to SEP holders occupying a dangerous position from the perspective of the antitrust laws: standards help coordinate disparate technologies and products from many firms into a consolidated, cohesive set. This enables interoperability, access, and the accumulation of massive network effects.144Given those valuable network effects, SEP holders who engage with the process of standards development and make FRAND commitments become ex post gatekeepers—regardless of their ex ante position in the market—to the implementation of standards and thereby control access to the entire market. If an SEP holder then violates its FRAND commitments by refusing to deal, the SEP holder has exhibited all of the markers of a Section 2 case that results in liability.

First, the SEP holder has acquired control over access to an essential facility (the relevant standard) and then denied competitors access to that facility (by refusing to license a patent necessary to fulfill the standard).145Although the same refusal to license its patent might have been acceptable if the SEP holder was not part of the SSO and the patent was not part of the standard, the market power and bargaining position of the patent holder is fundamentally altered when a patent becomes standard essential. This is reminiscent of Associated Press, except here the coordinating organization attempted to prevent the abuse of the SEP holder’s position by securing FRAND commitments from them.146It is therefore the deviant behavior of the SEP holder, not the SSO itself, that is to blame for the anticompetitive harm.

Second, the salient facts of a refusal to deal by an SEP holder are closely analogous to those of Aspen Skiing. The defendant monopolist was found liable in Aspen Skiing for two primary reasons: it had terminated a prior course of voluntary dealing and it had sacrificed short-run profits in order to harm a competitor.148Although an SEP holder may not have previously dealt with any given prospective standard implementer, the SEP holder’s participation in the SSO and its FRAND commitments constitute a prior course of dealing with allfellow participants and implementers of the standard. The subsequent violation of contractual FRAND commitments is a clear termination of that course of dealing. Additionally, licensing an SEP at a reasonable rate is, in isolation,obviously profitable for an SEP holder in the short-run (compared to an alternative world where the SEP holder earns no licensing revenue). The failure to profitably license at a reasonable rate raises, as it did in Aspen Skiing, a strong inference that the goal of the refusal to deal is anticompetitive.149Even if the conduct in Aspen Skiingis at the outer edge of Section 2 liability, it still falls within the boundaries of Section 2 liability. A FRAND-violating refusal to deal by an SEP holder, resembling the important features of Aspen Skiingas closely as it does, must also fall within that boundary.150

Finally, the burden of an inquiry into the intent of the SEP holder should be exactly reversed from what it was when the circuit courts considered refusals to license intellectual property more broadly. In those circuit court cases, the business justifications of the rights holders were treated as presumptively valid and defensible in light of the point of the intellectual property laws. Rather than appearing to be anticompetitive on its face, a refusal to deal seemed well within the ambit of reasonable, legislatively-permitted behavior by a firm holding valuable patents or copyrights. But the inclusion of a patent in a standard is transformative for a firm, and the firm becomes something much more than just another intellectual property rights holder. At that point, the subsequent violation of FRAND commitments is actually anticompetitive on its face: it loudly proclaims that the SEP holder has recognized its power in the market and decided to turn that power toward damaging the competitive process that it had previously contracted to protect and promote. PATENTS1119The presumption of antitrust liability for a SEP holder suggests that it should be presumed to not have a valid business justification when refusing to deal. The SEP holder would have the burden of rebutting this presumption before the court and substantiating a legitimate, procompetitive business justification for the refusal to deal.

B.Contrary Considerations

The strongest counterargument against presumptive antitrust liability for SEP holders who violate their FRAND commitments with a refusal to deal—and against any version of the essential facilities doctrine—is based in the fear that this approach to competition policy would lead to reduced investment and innovation.152The general form of the argument is that forcing firms to deal with competitors might increase competition in the short-run, but in the long-run it will reduce the incentive to innovate153because innovative firms will know that they will not be able to fully capitalize on a successful investment.154This concern is particularly strong in the realm of intellectual property. After all, these rights were specifically developed to give innovators and creators the ability to exclude others from copying and devaluing their work.155This increases the value of intellectual property to the owner and, in turn, encourages the creation of more intellectual property. Without the power to exclude competitors, a patent holder would have very little reason to take the risks and make the investments needed in order to develop a new idea or technology.

However, arguments of this form are often true at the extreme but not necessarily correct at the margin.156The complete lack of protection for intellectual property rights would be devastating for creators and inventors and would drastically reduce the incentives to innovate. But this does not mean that reducing the protections for intellectual property will always reduce the incentives for innovation to a greater degree than it will have positive, structural effects on the market.157To the contrary, this Note argues that antitrust liability will have positive, structural effects on the market which benefit competition and innovation more than the reduced incentives will harm competition and innovation. Still, this debate is fertile ground for further discussion, inquiry, and empirical research. Another possible objection to antitrust liability—this time on statutory rather than policy grounds—is that the Patent Act158created immunity for unilateral refusals to license patents.159The Federal Circuit adopted a version of this approach in CSU v. Xerox. The court based its decision, in part, on an inference that, “[t]he patentee’s right to exclude is further supported by [S]ection 271(d) of the Patent Act.”160But this view is not widely held by academics,161other courts,162or the DOJ or FTC.163A full examination of the Patent Act is outside the scope of this Note, but the idea that § 271(d) created broad antitrust immunity for intellectual property owners is a relatively fringe view.

Finally, it could be argued that the Supreme Court has recently expressed a reluctance to endorse either the essential facilities doctrine or the logic of Aspen Skiing. So, a new presumption of antitrust liability grounded in their fruitful combination is extremely unlikely in the near term. This argument is probably correct. But the question of what the law affords and what should be done with that affordance is separate from the question of what a particular court is likely to do. Presumptive antitrust liability for SEP holders may be wise today, unlikely tomorrow, and a reality the day after.

IV.CONCLUSION

This Note does not argue that an SEP holder should be prevented from benefiting when its patents lend value to a standard; this Note argues that an SEP holder should be prevented from benefiting when it attempts to abuse its position as a gatekeeper to a vital, collaborative standard. A presumption of antitrust liability for an SEP holder who refuses to deal in violation of its FRAND commitments accomplishes this balance. In some dynamic markets, the returns to innovation and the cycle of creative destruction are enough to ensure competition and progress.164But in standards-driven markets that derive their value from the coordinated creation of networks, the antitrust laws are an important bulwark of continued competition and growth.165They should be used accordingly. 164See Katz & Shelanski, supra note 156,at 5 (“Creative destruction means that a firm’s acquisition of possession of market power may be fleeting and that firms must protect such power through ongoing innovation efforts. Under constant pressure from actual and potential innovators, the incumbent firm itself produces better products on better terms for consumers....”). 165See Lao, supra note 22,at 562 (“Combined with a closed network system, network effects can, therefore, effectively create or reinforce existing entry barriers, insulate the monopolist from competition, and lock consumers into the existing technology.”).

#### Only antitrust effectively deters holdup because of treble damages

Tsilikas 17, \*Haris Tsilikas is an IP and Antitrust Consultant, a Doctoral Candidate and Visiting Research Fellow at the Max Planck Institute for Innovation and Competition, Munich; (2017, Antitrust Enforcement and Standard Essential Patents: Moving beyond the FRAND Commitment”, https://www.jstor.org/stable/pdf/j.ctv941t01.9.pdf?refreqid=excelsior%3A92dc720d1ebc7088811b40032a60f575)

Antitrust could play a meaningful role.165 The most important contribution of antitrust enforcement against abuses of SEPs is its deterrent effect.166 Although patent law reforms or contractual binding of subsequent SEPs-holders to FRAND licensing would provide to victims of hold-up useful defences in court, they do not sufficiently deter abusive assertion of SEPs in the first place. For instance, the contractual binding to FRAND could raise counterclaims of breach of contract or/and contractual performance; however, the opportunistic SEP-holder will, in case it loses on such grounds, be left no worse than with a licence on FRAND terms. In the end, a patent hold-up is indeed precluded, but contractual constraints can do little to prevent opportunistic assertion of SEPs in the first place. The victims still suffer the costs of uncertain and resource-draining litigation; most importantly, the reliability of the standards-setting process might still be at risk.

Antitrust enforcement on the other hand, in imposing tortfeasors positive monetary losses in the form of fines, alters the profit-cost calculus of opportunistic behaviour in the first place; opportunistic assertion of SEPs will come at a cost. Of course, a too-heavy-handed approach could have a chilling effect on legitimate patent assertions against implementers that are reluctant to pay FRAND royalties, thus leading to false positives. Antitrust enforcement should carefully examine the specificities of each case, such as the particular PAE conduct, the relationship between PAEs and practicing entities, the structure of downstream markets.167 More importantly, an economically informed antitrust analysis focusing on the actual and potential anticompetitive effects of opportunistic SEPs assertion should prohibit behaviour that is truly harmful to consumers. Safeguarding the inclusive and efficient character of the standards-setting process is a competition law problem. Informed antitrust analysis could provide adequate responses to opportunistic PAE behaviour and privateering.

#### Private action fails and result in direct monopoly outcomes.

Melamed & Shapiro 18, \*A. Douglas Melamed is Professor of the Practice of Law at Stanford Law School; \*Carl Shapiro is the Transamerica Professor of Business Strategy at the Haas School of Business at the University of California at Berkeley; (May 2018, “How Antitrust Law Can Make FRAND Commitments More Effective”, <https://www-cdn.law.stanford.edu/wp-content/uploads/2018/05/How-Antitrust-Law-Can-Make-FRAND-Commitments-More-Effective.pdf>)

2. Why Antitrust Enforcement Is Necessary

Some SSO members have an interest in ensuring that the SSO takes steps to minimize the potential harms from the SEP holders’ monopoly power, and this undoubtedly explains in part why most SSOs have adopted FRAND policies or similar requirements. But, as shown in the economic model in the Appendix,73 SSOs cannot in general be counted on to adopt effective FRAND policies. The bases for this conclusion, which is central to our argument for the applicability of Section 1 to SSO FRAND rules, can be summarized as follows.74

First, the SSO members collectively have an interest in permitting SEP holders to charge supracompetitive royalties that elevate the downstream price of compliant devices to the monopoly level. Doing so will enable the members in aggregate to collect increased revenues from consumers, and thus to generate increased profits that in theory could be shared by all the members. In other words, supracompetitive royalties can enrich industry participants as a group at the expense of final consumers. This fact alone should serve as a clear and strong signal regarding the dangers of counting on SSOs to implement effective FRAND policies: if the SSO members negotiate efficiently, the outcome will be just as bad for consumers as if the members agreed to fix downstream prices.75 The fundamental problem is that final consumers are not at the table when the SSO rules are negotiated.

Second, SSO members that own SEPs but earn little or no profits as implementers have a powerful self-interest in being able to exercise the ex post monopoly power associated with their SEPs. Because SSO policies are usually determined by a consensus process, these members will likely be able to block the adoption of fully effective FRAND policies. Moreover, these SSO members often have the greatest interest in SSO patent policies. Since much of their income may be attributable to patent licensing, they can be expected to devote substantial resources to block the adoption of FRAND policies that effectively prevent patent holdup.

Third, even SSO members that earn significant profits as implementers may have mixed incentives if they also own SEPs, which can also lead to weak or in-effective FRAND rules. In the Appendix, we show that, if the requisite share of votes in the SSO are cast by firms whose share of SEP royalties is at least as large as their share of downstream profits, and if these firms can coordinate their voting over the FRAND rules, then an SSO unconstrained by antitrust laws will establish FRAND rules leading to an outcome no better for consumers than would result from an integrated monopolist controlling all SEPs and all downstream sales.76

Fourth, even SSO members that are downstream implementers and own few, if any, SEPs may have only a modest interest in promoting effective policies to restrict ex post opportunism. Because all implementers will be subject to the opportunism, all of them will face increased licensing costs, and therefore will likely be able to pass on most or all of the increased costs to their customers.77 Furthermore, these implementers might not be especially active or effective in the standard-setting process for free-riding or public-good reasons, especially if SEP royalties constitute only a relatively small portion of the costs of their standard-implementing products. Public choice theory predicts that the highly motivated SEP holders are likely to have the greatest influence over patent policies.

Empirical evidence bears out these concerns. As a starting point, we find it striking that SSO FRAND rules are almost always quite vague.78 Notably, SSOs in which SEP holders are more prevalent tend to have weaker FRAND rules.79 Further, to our knowledge, SSOs have made almost no effort to enforce their FRAND rules and have, instead, left enforcement efforts to others.80 This evidence raises serious doubts about the effectiveness of the existing FRAND rules in preventing ex post opportunism.

#### Holdup is real – neg studies are structurally flawed and funded by Qualcomm

Shapiro 20, \*Carl Shapiro is the Transamerica Professor of Business Strategy Emeritus at the Haas School of Business, University of California at Berkeley; \*Lemley is the William H. Neukom Professor at Stanford Law School and a partner at Durie Tangri LLP; (2020, “THE ROLE OF ANTITRUST IN PREVENTING PATENT HOLDUP”, https://faculty.haas.berkeley.edu/shapiro/patentholdup.pdf)

C. Actual Patent Holdups Are Very Difficult to Measure

As with holdup in general, quantifying the frequency and magnitude of actual patent holdups is very difficult as a practical matter and not a useful way of assessing the importance of the patent holdup problem. Rarely can researchers observe the ex post price, because patent licensing terms are normally confidential. Even when researchers can observe the license fees, they are often embedded in a complex agreement. And even in those rare cases where researchers can accurately observe the ex post price, they are unlikely to observe the ex ante price, making it difficult if not impossible to measure the magnitude of the holdup.

Litigated cases also are problematic as a source of data to quantify the magnitude of actual patent holdups. A litigated case resulting in an award of reasonable royalties may well involve attempted holdup, but by definition it cannot provide smoking-gun evidence of actual holdup, at least if one accepts that the royalties awarded by the court are reasonable.64 Rather, at least since the Supreme Court eliminated the automatic entitlement to an injunction, litigation to judgment (which is rare) often reflects a refusal to give in to holdup by a defendant willing to take its chances in court. And the vast majority of patent cases settle. The terms of a settlement are rarely observable, so it is impossible to know whether those settlements reflected the value of holdup.

Notwithstanding these points, a number of authors have pointed to a lack of empirical evidence to argue that patent holdup either does not exist or is not a significant problem.65 Even taken on their own terms, many of these papers are deeply flawed. One such paper, which has often been cited by those who downplay the importance of patent holdup, purports to offer empirical evidence inconsistent with the hypothesis that SEP holdup has slowed innovation or harmed consumers.66 The conclusion to this Qualcomm-funded paper states, “[w]e cannot reject the hypothesis of no SEP holdup.”67 How do these authors reach this conclusion? They compare rates of change of quality-adjusted prices in “SEP- reliant” industries with “similar” non-SEP-reliant industries, primarily over the 1997-2013 period.68 For example, they show that quality-adjusted prices of cellular phones have fallen faster than the quality-adjusted prices of automobiles.69 This exercise does not address the relevant hypothesis: whether SEP holdup increased the price of cellular phones from what it otherwise would have been.70 The quality- adjusted prices of pharmaceuticals have risen much faster than automobiles over the same period of time, but that similarly is not proof that pharmaceuticals are subject to a patent holdup problem.

Beyond the obvious and fatal flaws in this empirical work,71 the whole line of inquiry is of limited relevance for the purpose of measuring the social costs of holdup or designing institutions to limit patent holdup, because it only looks for instances of actual patent holdup. As explained above, these instances are very difficult to detect and are only the tip of the iceberg in terms of the social costs of patent holdup.72 So far as we can tell, the vast majority of these papers have been funded by Qualcomm and other patent holders seeking to weaken the institutions designed to control patent holdup, increase their leverage in licensing negotiations, and thus increase their ability to monetize their patents.73

Despite the difficulties of observing the incidence and magnitude of actual patent holdups, we are able to observe the telltale signs of actual patent holdup. Transaction cost economics, and simple bargaining theory for that matter, tell us that actual patent holdup can be expected to occur when three conditions are present: (1) a firm has developed a new product independently; (2) that firm has made significant investments that are specific to one or more patents asserted against that product; and (3) the firm is not protected from patent holdup.74 As discussed above, conditions (1) and (2) are common in the high-tech sector, placing considerable weight on the institutions that protect firms from patent holdup.

The presence of those institutions is itself evidence that the patent holdup problem is real and significant. As we noted in Part I, companies try to structure their transactions to avoid holdup, developing institutions for that purpose. As we have seen, the traditional market solutions do not work well for patents. In most industries, the central mechanisms limiting patent holdup come from patent law, namely the rules governing injunctions and patent damages. In the high-tech sector, companies have overwhelmingly turned to SSOs in an effort to obtain global commitments to an ex ante royalty, which appear in the form of FRAND commitments. The near-universal recognition in the industry of the need for such a mechanism is strong evidence that companies view holdup as a problem they must build institutions to avoid.

#### Present tech innovation is inefficient AND useless.

Ashish Arora et al. 20, Senior Associate Dean for Strategy. Rex D. Adams Professor of Business Administration, Fuqua School of Business, Duke University; Sharon Belenzon, Professor, Strategy, Fuqua School of Business, Duke University. Research Associate, National Bureau of Economic Research; Andrea Patacconi, Professor, Strategy, Norwich Business School; Jungkyu Suh, PhD, Business, Duke University, "The Changing Structure of American Innovation: Some Cautionary Remarks for Economic Growth," Innovation Policy and the Economy, Vol. 20, 2020, NBER.

A defining feature of modern economic growth is the systematic application of science to advance technology. Many innovations that spurred economic growth in the twentieth century, including synthetic fibers, plastics, integrated circuits, and gene therapy, originated from advances in the natural sciences, engineering, and medicine. Science, by producing “a potential for technology far greater than existed previously,” clearly distinguishes modern economic growth from previous economic epochs (Kuznets 1971).

However, despite sustained increases in the quantity of scientific knowledge, productivity growth in most advanced economies has stagnated in recent decades in comparison to a “golden age” in the mid-twentieth century. Using data from the United States, Gordon (2016) shows that real gross domestic product (GDP) per hour (i.e., labor productivity) grew substantially in the middle of the twentieth century, from 1.79% per year between 1870 and 1920 to 2.82% per year between 1920 and 1970. However, in the most recent period (1970–2014), productivity grew by a modest 1.62% per year. Gordon concludes that productivity rose between 1920 and 1970 largely because of significant technological progress, but more recently technical advance has been much less potent in spurring growth. This slowdown is surprising given the sustained expansion of scientific input (measured in terms of research dollars spent) and output (measured by academic articles published) from American academia, as shown in figure 1.1

Chart

Description automatically generated

Gordon (2016) attributes the rapid pace of technological progress between 1920 and 1970 to the development and extension of earlier fundamental technologies, such as the internal combustion engine and electricity. This process, which was often accompanied by important advances in science and engineering, was largely carried out by researchers working in corporate labs, which by the 1920s had replaced individual entrepreneurs as the primary source of American invention. As Gordon writes:

Much of the early development of the automobile culminating in the powerful Chevrolets and Buicks of 1940–41 was achieved at the GM corporate research labs. Similarly, much of the development of the electronic computer was carried out in the corporate laboratories of IBM, Bell Labs, and other large firms. The transistor, the fundamental building block of modern electronics and digital innovation, was invented by a team led by William Shockley at Bell Labs in late 1947. The corporate R&D division of IBM pioneered most of the advances of the mainframe computer era from 1950 to 1980. Improvements in consumer electric appliances occurred at large firms such as General Electric, General Motors and Whirlpool, while RCA led the early development of television.

(Gordon 2016, 571–72)

By the 1980s, however, many corporations began to look to universities and small start-ups for ideas and new products.2 Large corporations’ reliance on externally sourced inventions grew, and many leading Western corporations began to withdraw from scientific research (Mowery 2009; Arora, Belenzon, and Patacconi 2018). Some corporate labs were shut down and others spun off as independent entities. Bell Labs had been separated from parent company AT&T and was placed under Lucent in 1996; Xerox PARC had also been spun off into a separate company in 2002. Others had been downsized: IBM under Louis Gerstner redirected research toward more commercial applications in the mid-1990s (Bhaskarabhatla and Hegde 2014).3 A more recent example is DuPont’s closing of its Central Research and Development Lab in 2016. Established in 1903, DuPont research rivaled that of top academic chemistry departments. In the 1960s, DuPont’s central research and development (R&D) unit published more articles in the Journal of the American Chemical Society than Massachusetts Institute of Technology (MIT) and California Institute of Technology (Caltech) combined. However, in the 1990s, DuPont’s attitude toward research changed and after a gradual decline in scientific publications, the company’s management closed its Central Research and Development Lab in 2016.4

These examples are backed by systematic evidence. National Science Foundation (NSF) data indicate that share of research (both basic and applied) in total business R&D in the United States fell from about 30% in 1985 to below 20% in 2015 (fig. 2). The figure also shows that the absolute amount of research in industry, after increasing over the 1980s, barely grew over the 20-year period between 1990 and 2010. Other data show the same decline. Utilizing data on scientific publications, Arora et al. (2018) show that the number of publications per firm fell at a rate of 20% per decade from 1980 to 2006 for R&D performed in American listed firms. The authors also find that the drop is even more dramatic for established firms in high-quality journals. For articles within the top quartile of journal impact factor scores, the magnitude of the drop increases to more than 30%. Large firms’ withdrawal from science can also be gleaned from the list of R&D 100 awards winners. Fortune 500 firms won 41% of the awards in 1971 but only 6% in 2006 (Block and Keller 2009). Over the same period, total industry R&D and patenting grew steadily, as did university-performed research (see fig. 6). This evidence points to the emergence of a new division of innovative labor, with universities focusing on research, large firms focusing on development and commercialization, and spin-offs, start-ups, and university technology licensing offices responsible for connecting the two.

Chart, histogram

Description automatically generated

#### Startups and venture capital are decreasing now

**Nadler, 20** (Jerrold Nadler, Chairman, Comittee on the Judiciary, 20, accessed on 8-22-2021, Judiciary.house, "SUBCOMMITTEE ON ANTITRUST, COMMERCIAL AND ADMINISTRATIVE LAW", https://judiciary.house.gov/uploadedfiles/competition\_in\_digital\_markets.pdf?utm\_campaign=4493-519)//Babcii

In recent decades, however, there has been a sharp decline in new business formation as well as early-stage startup funding.169 The number of new technology firms in the digital economy has declined,170 while the entrepreneurship rate—the share of startups and young firms in the industry as a whole—has also fallen significantly in this market.171 Unsurprisingly, there has also been a sharp reduction in early-stage funding for technology startups.172 The rates of entrepreneurship and job creation have also declined over this period. The entrepreneurship rate—defined as the “share of startups and young firms” in the industry as a whole— fell from 60% in 1982 to a low of 38% as of 2011.173 As entry slows, the average age of technology firms has skewed older.174 Job creation in the high-technology sector has likewise slowed considerably.175 In 2000, the job creation rate in the high-technology sector was approaching 20% year-over-year. Within a decade, the rate had halved to about 10%.176 Although the job creation rate in the high-technology sector has fallen substantially since the early 2000s, the job destruction rate in 2011 was roughly unchanged from 2000.177 As a result, in 2011 the rate of job destruction in the high technology sector was higher than the rate of job creation, a reversal from the year 2000, when the jobcreation rate far outpaced the job-destruction rate.178 In line with this trend, there is mounting evidence that the dominance of online platforms has materially weakened innovation and entrepreneurship in the U.S. economy.179 Some venture capitalists, for example, report that they avoid funding entrepreneurs and other companies that compete directly with dominant firms in the digital economy.180

# 2AC

## Case

### Adv 1

#### Holdup is real and empirical – consensus goes aff

McSweeny 18 [Terrell, Ex-Commissioner of FTC (held position when written), “Holding the Line on Patent Holdup: Why Antitrust Enforcement Matters Commissioner Terrell McSweeny”. 3/21/18. https://www.ftc.gov/system/files/documents/public\_statements/1350033/mcsweeny\_-\_the\_reality\_of\_patent\_hold-up\_3-21-18.pdf]

Recently, some academics and practitioners have suggested that patent holdup is a “flawed” theory without real-world evidence to back it up. 2 It has also been suggested that recent empirical studies “contradict” patent holdup.3 I do not find these arguments compelling. The competitive risks associated with patent holdup have long been an area of bipartisan agreement – for good reason. It would be unfortunate if the antitrust agencies were to unlearn the lessons of over 15 years of scholarship and dbipartisan study and question their longstanding support for combatting holdup based on vague concerns about over-deterrence. In 2001, Tim Muris announced an initiative by the Federal Trade Commission and Department of Justice to “develop a better understanding of how to manage the issues at the intersection of competition and intellectual property law and policy.”4 Then-Chairman Muris identified the standard-setting process as an important topic for further study. The antitrust agencies held a series of hearings that featured over 300 panelists and more than 100 written comments. Based on that record, as well as a review of the scholarly literature, in April 2007, 1 The views expressed in this statement are my own and do not necessarily reflect those of the Federal Trade Commission or any other Commissioner. 2 See, e.g., Feb. 13, 2018 Letter to Assistant Attorney General Makan Delrahim, https://cpip.gmu.edu/wpcontent/uploads/sites/31/2018/02/Letter-to-DOJ-Supporting-Evidence-Based-Approach-to-Antitrust-Enforcementof-IP.pdf. See also Makan Delrahim, Assistant Attorney General, Dep’t of Justice, The “New Madison” Approach to Antitrust and Intellectual Property Law, Remarks at U. Penn. Law School, Philadelphia, PA (Mar. 16, 2018), https://www.justice.gov/opa/speech/file/1044316/download (claiming that holdup theories “remain an empirical enigma in the academic literature” and that holdup “is fundamentally not an antitrust problem.”) 3 See Feb. 13, 2018 Letter to Assistant Attorney General Makan Delrahim, supra note 2. 4 Tim Muris, Competition and Intellectual Property Policy: The Way Ahead, Prepared Remarks before the American Bar Association, Antitrust Section Fall Forum, Nov. 15, 2001, https://www.ftc.gov/publicstatements/2001/11/competition-and-intellectual-property-policy-way-ahead. 2 the agencies issued a joint report, “Antitrust Enforcement and Intellectual Property Rights: Promoting Innovation and Competition.”5 The agencies’ 2007 Report devoted over 20 pages to discussing the patent “holdup problem.” Numerous panelists raised the issue of patent holdup, including industry participants speaking from real-world experience. 6 The Report noted that this problem threatens harm to consumers both through higher prices as well as “less investment in developing and implementing standards.”7 The agencies closely analyzed several mechanisms that could assist standard-setting organizations (SSOs) in “mitigat[ing] the threat of licensing hold up” to avoid these anticompetitive outcomes.8 The agencies’ joint findings were the result of careful and thorough analysis of antitrust and intellectual property issues. The Commission ultimately voted unanimously (5-0) to approve the findings of the Report. In 2011, a subsequent Commission again voted unanimously (5-0) to endorse a report on “The Evolving IP Marketplace,” which noted that “[h]old-up in the standard setting context can be particularly acute.”9 The Theory of Patent Holdup The theory of patent “holdup” is simple and straightforward. It refers to the fact that the bargaining position of a patent-holder may increase considerably after a patent is included in the standard. The patent holder may use this position as leverage to cause a licensee to pay up to the value of switching to non-standardized technology. The agencies’ 2007 Report explains the holdup problem as follows: In the standard-setting context, firms may make sunk investments in developing and implementing a standard that are specific to particular intellectual property. To the extent that these investments are not redeployable using other IP, those developing and using the standard may be held up by the IP holders. 10 Oliver Williamson won the Nobel Prize in economics in 2009 due in no small part to his work showing how opportunistic behavior such as holdup can lead to inefficient economic outcomes.11 As Dennis Carlton has explained, once a patent is included in a standard, “the patent owner definitely has some additional market power conferred on him that he can exploit in the absence of a constraint on him.”12 That added market power derives from the value of the standard itself, rather than the value of the underlying intellectual property.13 This is what makes holdup economically inefficient. There is nothing novel about the theory of patent holdup in the standard-setting context. Indeed, the agencies’ 2007 Report explains that it is merely “a variant of the classic ‘hold-up problem.’”14 10 2007 Report, supra note 5, at 35 n.11. See also 38 (“A holder of IP incorporated into a standard can exploit its position if it is costly for users of the standard to switch to a different technology after the standard is set. Making such a change would require abandoning that standard and developing a new one, but developing an alternative standard could be costly and may delay the introduction of a new product. The profits lost by such a delay may represent a significant portion of the cost of developing the alternative standard. In addition, to implement an alternative standard for an existing product that requires compatibility and interoperability, the SSO members might incur switching costs in redesigning components that had been based on the old standard and might have to subsidize consumers’ migration from a standard based on one technology to a standard based on another technology.”). The Evidence on Patent Holdup There is ample evidence that patent holdup exists. The FTC has brought a number of enforcement actions challenging opportunistic behavior by patent holders designed to hold up implementers of a standard. Panelists at the FTC/DOJ hearings reported having experienced patent holdup. 15 There is also strong anecdotal support for the theory that patent holders are willing to seek considerably more than the FRAND value of their patents, consistent with the added market power conferred by inclusion within a standard. When courts have been asked to rule on the reasonableness of purported “FRAND” offers by patent holders, they have found patent holders demanding far more than that to which they were entitled – a finding consistent with holdup. Below are two recent examples: Microsoft Corp. v. Motorola, Inc. (W.D. Wash. Apr. 25, 2013): Motorola sought to exclude Microsoft’s gaming consoles from the United States and demanded that Microsoft pay royalties of between $6–8 per console for the use of patents reading on the 802.11 and H.264 standards. The court determined that the F/RAND rate was less than four cents per unit for the 802.11 standard, and less than one cent per unit for the H.264 standard. The cumulative RAND royalty found appropriate by the court was approximately 1/150th the royalty sought by Motorola.16 Realtek Semiconductor Corp. v. LSI Corp., (N.D. Cal. June 16, 2014): LSI filed an action with the U.S. International Trade Commission (ITC) seeking an exclusion order and then offered to license Realtek the underlying SEPs in exchange for a royalty that exceeded the selling price of Realtek’s standardcompliant products. The federal district court determined that the cumulative F/RAND royalty to which LSI was entitled was 0.19% of the selling price – less than 1/500th the amount that LSI had demanded17 In both cases, the F/RAND royalty rates offered by SEP-holders were orders of magnitude higher than what a neutral arbitrator found to be fair and reasonable. It is also worth noting that 15 See, e.g., note 6 supra. 16 Microsoft Corp. v. Motorola, Inc., 2013 U.S. Dist. LEXIS 60233\* 303 (W.D. Wash. Apr. 25, 2013). The cumulative royalty of 4.026 cents was 1/149th the FRAND rate sought by Motorola. The court also calculated ranges of RAND rates. The sum of the “upper bound” of these ranges was just under 36 cents. This upper bound was still less than 1/16th of the FRAND rate sought by Motorola. 17 Realtek Semiconductor Corp. v. LSI Corp., 2014 U.S. Dist. LEXIS 81673 \* 23 (N.D. Cal. June 16, 2014). 5 the SEP holders sought exclusion orders, which would have operated in much the same way as an injunction by limiting the sale of the implementing products in the United States. Critics of antitrust enforcement in the holdup context sometimes point to studies showing that quality-adjusted prices have decreased in high-tech industries where standard-setting is common. 18 These studies do not actually “contradict” the theory of patent holdup. The question is not whether quality-adjusted prices will decrease at all, but whether holdup slows the pace of this trajectory for new technologies. Imagine a construction project that closes a lane of traffic on a busy roadway. Cars will continue to move while construction is underway – just more slowly. The mere fact that cars are still moving forward does not “contradict” the notion that construction impedes traffic. Similarly, here, the fact that quality-adjusted prices are still “moving forward,” by itself, provides little useful information about the effect of patent holdup on the pace of innovation or on consumer prices. It would be difficult to design a study that would provide a conclusive empirical answer one way or the other given the inherent unknowability of the but-for world. In the absence of such an answer, do we heed the straightforward economic theory on holdup, or do we ignore it? Do we recognize the compelling anecdotal evidence of patent holdup, or do we ignore that too? My recommended approach is the same one the agency has been following for the better part of two decades – we should recognize the potential for harm from holdup and enforce on a case-by-case basis where appropriate.19 18 See, e.g., February 13, 2018 Letter to Assistant Attorney General Makan Delrahim, supra note 2 (“Several empirical studies demonstrate that the observed pattern in high-tech industries, especially in the smartphone industry, is one of constant lower quality-adjusted prices, increased entry and competition, and higher performance standards. These robust findings all contradict the testable implications of ‘patent holdup’ theory.”). 19 Some have suggested that the antitrust agencies should focus more attention on so-called patent holdout. Attempts to draw an equivalence between holdup and holdout are misguided and ignore the underlying reason for focusing on patent holdup as antitrust enforcers – namely that adoption of a standard locks in implementers and confers incremental market power on one side of a licensing negotiation. Antitrust enforcers would, of course, take seriously any evidence of collusion by implementers to engage in collective holdout against a patent holder. 6 Conclusion The FTC’s record of challenging holdup on antitrust grounds stretches back over two decades.20 The Agency has brought seven significant enforcement actions across both Republican and Democratic administrations.21 The good news is that the standard-setting process works well overall. These seven challenges were brought against a backdrop of hundreds of thousands of FRAND licensing negotiations. Parties successfully negotiate the vast majority of SEP licenses without involvement from the courts or antitrust agencies. Although antitrust enforcement actions are rare, they are nonetheless important.22 For example, between 1996 and 2003, the FTC brought three cases challenging deception by patent holders for failure to disclose patents reading on standards. Following these enforcement actions, this type of opportunistic behavior appears to have abated. By protecting the integrity of the standard-setting process itself, sound antitrust enforcement actually strengthens market opportunities for new technologies, thus improving the incentive for valuable innovation. The motivation for firms to engage in holdup will endure where there is opportunity. Given the importance of standard-setting to the modern economy, it is imperative that the FTC continue to take holdup seriously and not abdicate its antitrust enforcement mission in this area.

#### Much of holdup evidence is hidden from the public eye – thousands of deals are made behind closed doors

Wood 13 [Chris Wood and Joseph Kattan, partners in the Antitrust and Trade Regulation practice of Gibson, Dunn & Crutcher LLP. “Standard-Essential Patents and the Problem of Hold-Up”. 12/13/13. http://awa2014.concurrences.com/IMG/pdf/standard\_essential\_patent\_kattan-wood.pdf]

It is notable that the standard implementers in the cases discussed above were large multinational corporations, with the resources to engage in protracted litigation. Less known are the financial settlements extracted by holders of FRAND-encumbered SEPs, which are subject to confidentiality agreements that shield them from the public eye. For example, before having to defend its royalty demands in a declaratory judgment action, Innovatio had sent 8,000 demand letters to businesses such as coffee shops and hotels that used Wi-Fi equipment.46 The terms of its settlements with these businesses are not known. Nor are the terms of the confidential settlements of infringement cases brought by SEP holders known. The size of the demands made by the SEP holders in the cases discussed above certainly supports the view that implementers of industry standards face a genuine risk of post-adoption patent hold-up. Particularly in the case of Wi-Fi patents, which were at issue in each of these cases, the demands are extraordinary not only because of the royalty stack that they imply but because each involved a small sliver of the universe of SEPs for a standard for which the “central elements” were based on publicly available technologies.

#### First mover advantage locks in patent holder participation and innovation

Stern 18, \*Richard H. Stern, Professorial Lecturer in Law, The George Washington University Law School. A Washington, D.C. patent and antitrust attorney, Stern was Chief of the Patent Section of the US Justice Department’s Antitrust Division during the Nixon and Ford Administrations; (2018, “Who Should Own the Benefits of Standardization and the Value It Creates?”, https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1439&context=mjlst)

D. INCENTIVIZE ME OR I’LL DEFECT

A highly theoretical argument is often made by SEP owner spokesmen—that lessened compensation to SEP owners will “disincentivize” them from creating technology and contributing it to standardization, stagnating further standardization. For example:

If the SEP holder cannot capture any of the value from standardization that its technology creates for the standard, it will have a dampened incentive to continue contributing its best technologies to SSOs. In the long run, the quality of technologies contributed to a future standard—and the expected value of that new standard—would decrease. The SEP holder’s decision to contribute its technologies to a standard depends on the compensation that an SEP holder expects to obtain from such a contribution, compared with the SEP holder’s alternative option to monetize its invention outside the standard. . . . If the SEP holder expects not to be compensated fully for its contributions, it will not commit its most valuable technologies to the standard.431

But the amount of dampening of incentive (assuming that we do not already have enough or more than enough incentive for smartphones) may well be outweighed in impact by the prospect of nonetheless gaining first-user and head-start advantage from incorporation of one’s technology into a standard, and the opportunity to increase one’s equipment sales (anointed with the imprimatur of the standard),432 even if one cannot also obtain monopoly profits as well, from SEP royalties. In a sense, those advantages are a form of “the compensation that an SEP holder expects to obtain” from such a SEP contribution, but the commentator fails to take those significant incentives into consideration.433 Moreover, the supposed “SEP holder’s alternative option to monetize its invention outside the standard” may be a figment of the SEP holder spokesman’s imagination.434 If an alternative technology becomes standard, the only opportunity to monetize the withheld invention may be to incorporate the technology into unsaleable non-standard products. Defection may be a poor business strategy.

#### Empirically disproven

Stern 18, \*Richard H. Stern, Professorial Lecturer in Law, The George Washington University Law School. A Washington, D.C. patent and antitrust attorney, Stern was Chief of the Patent Section of the US Justice Department’s Antitrust Division during the Nixon and Ford Administrations; (2018, “Who Should Own the Benefits of Standardization and the Value It Creates?”, https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1439&context=mjlst)

Furthermore, a considerable amount of standardization activity has been coming from groups that prohibit the participating companies or individuals from collecting SEP royalties—so-called “RF-RAND” (royalty-free RAND)435 and “RAND-Zero” (RAND with zero royalties) groups or groups that rely on promises not to assert essential-patent claims436—as well as from SSOs that permit RAND licensing but whose members in practice collect royalties on few, if any, standards.437 The availability of these important, royalty-free technology sources is a factor in evaluating the threatened “disincentivization” and massive resistance against the policies reflected in the IEEE 2015 Patent Policy update.

Finally, the disincentivization argument is pure ipse dixit, for no analysis of comparative rates of return on alternative investment opportunities is offered. Nor is any empirical support provided.438 The rhetoric of “Incentivize me or I’ll defect” is completely unsupported and therefore not credible.

#### Studies prove even full patent invalidation triggers innovation increases - ICT and biotech are distinct

Galasso 14 [Alberto Galasso, Professor of Strategic Management at the University of Toronto. Mark Schankerman, Professor of Economics @ London School of Economics, Research Fellow at the Centre for Economic Policy Research. “PATENTS AND CUMULATIVE INNOVATION: CAUSAL EVIDENCE FROM THE COURTS”. June 2014. https://www.nber.org/system/files/working\_papers/w20269/w20269.pdf]

Second, we find that the impact of patent invalidation on subsequent innovation is highly heterogeneous. For most patents, the marginal treatment effect of invalidation is not statistically different from zero. The positive impact of invalidation on citations is concentrated on a small subset of patents which have unobservable characteristics that are associated with a lower probability of invalidity (i.e., stronger patents). There is also large variation across broad technology fields in the impact of patent invalidation and the effect is concentrated in fields that are characterized by two features: complex technology and high fragmentation of patent ownership. This finding is consistent with predictions of the theoretical models that emphasize bargaining failure in licensing as the source of blockage. Patent invalidation has a significant impact on cumulative innovation only in the fields of computers and communications, electronics, and medical instruments (including biotechnology). We find no effect for drugs, chemicals, 4 or mechanical technologies. Moreover, for two of the technology fields we study — medical instruments and drugs — we are able to construct alternative measures of cumulative innovation that exploit data on publicly-disclosed new product developments. The results confirm our findings using citations: patent invalidation has a significant effect on later innovation in medical instruments but no effect in pharmaceuticals.

## States

### 2AC – States

#### CP is preempted – federal and state lockout are equivalent

Samp 14—Richard A. Samp, Chief Counsel, Washington Legal Foundation (“The Role of State Antitrust Law in the Aftermath of *Actavis*,” *Minnesota Journal of Law, Science & Technology*, Vol. 15, No. 1, Article 14, https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1062&context=mjlst)

As noted above, there is precedent for a finding that state antitrust law is preempted to the extent that it conflicts with the policy underlying a federal statute.76 Moreover, in the context of patent law, federal courts have not hesitated to preempt state laws that the courts deem to stand as an obstacle to accomplishing Congress’s objectives (i.e., encouraging efforts to develop new and useful products).77 To the extent that any portions of Actavis’s holding can be deemed to reflect the Court’s perception of Congress’s new-product-development objectives, a state law is preempted if it is inconsistent with that holding and seeks to impose a greater degree of antitrust liability on the parties to a reverse payment settlement.

Actavis’s treatment of settlements involving a compromise entry date appears to meet that description. Actavis held that federal antitrust liability could not arise from a settlement in which the generic manufacturer agrees not compete for a number of years and in return is rewarded with an exclusive license to market its product several years in advance of the patent’s expiration date.78 Accordingly, states are not permitted to impose antitrust liability under similar circumstances because doing so would upset the balance that, according to Actavis, Congress sought to achieve between antitrust and patent law.

#### Standard setting is global and SSOs are outside of US jurisdiction

Kasdan 19 [Abraham and Michael. Partners in IP Law @ Wiggins and Dana LLP. “Recent Developments In The Licensing Of Standards Essential Patents”. 8/30/19. https://www.natlawreview.com/article/recent-developments-licensing-standards-essential-patents-0]

Technologies that operate across many different devices and geographical regions are all around us. As one example, today's mobile telephones can connect to 3G/4G/LTE and WiFi networks and communicate with other devices virtually anywhere in the world. This is made possible because all of these devices comply with highly specific technical standards that are promulgated by national and/or international standards setting organizations (SSOs), made up of companies involved in developing and building these global technologies.

When aspects of technical standards are protected by patents, the patent owners are generally obligated by the pertinent SSO to offer licenses to their patented technology under "fair, reasonable and non-discriminatory" (FRAND) terms, as the quid pro quo for having their patented technology included in the standard. The purpose behind the FRAND requirement is to prevent patent owners from gaining an unfair advantage over companies who must make devices that practice the standard in order to participate in the market; and are therefore necessarily “locked in” to standard-compliant designs.

Over the past several years, the licensing and litigation landscape involving standard essential patents (SEPs) and FRAND has become a matter of intense focus. Numerous technology industries, as well as courts around the world have begun to grapple with key issues such as “How do you determine what a FRAND licensing rate should be?” and whether a licensor’s offer is FRAND or not. This article summarizes several recent developments in the transnational licensing of SEP portfolios.

The Overall Landscape

Not surprisingly, most of the recent licensing disputes over SEPs involve the worldwide telecommunications industry. A host of multinational companies have been involved in developing the 2G, 3G, 4G and soon-to-be-commercialized 5G standards (aspects of which are also described by a bewildering array of acronyms, such as "LTE" and "LTE Advanced" ) These standards specify the technical features included in mobile phones and their networks.

The European Telecommunications Standards Institute (ETSI) is an SSO charged with developing worldwide standards for these technologies. Early on, SSOs recognized that the incorporation of patented technology into a standard could give the patent holder significant leverage when negotiating licenses. SSOs therefore required the patent holder to agree to make its SEPs available on FRAND licensing terms. However, ETSI, like other SSOs, does not provide guidance on how to structure licensing terms that meet the FRAND requirement. Indeed, doing so or setting price or royalty rates among entities in a given industry may raise antitrust issues. This leaves it to others to work out the specifics of how SEP owners can comply with the FRAND requirement.

#### Gets preempted

O’Rourke 10 [Ken, Senior Partner @ O'Melveny & Myers LLP. “United States: The FTAIA In State Court: A Defense Perspective”. 3/3/10. https://www.mondaq.com/unitedstates/trade-regulation-practices/95030/the-ftaia-in-state-court-a-defense-perspective]

A threshold question is whether these limitations similarly restrict the extraterritorial application of state antitrust laws. Defendants will argue that the state antitrust laws cannot permissibly extend to reach conduct or give rise to damages that Congress has placed beyond the reach of federal antitrust law under the FTAIA.

The defendants' argument goes like this. First, under the Supremacy Clause of the U.S. Constitution,4 federal law preempts state law even in the absence of an express preemption provision when, "under the circumstances of [a] particular case, [the challenged state law] stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."5

Second, the FTAIA's legislative history establishes that Congress had multiple objectives when enacting the statute. One objective was to ensure that the risk of Sherman Act liability did not prevent American exporters and other firms doing business abroad from entering into advantageous "business arrangements (such as joint selling arrangements), however anticompetitive, as long as those arrangements adversely affect only foreign markets."6

Another objective was to eliminate "ambiguity in the precise legal standard to be employed in determining whether American antitrust law is to be applied to a particular transaction."7

Congress sought to adopt a "clear benchmark ... for businessmen, attorneys and judges as well as [U.S.] trading partners"8 with the "ultimate purpose" of "promot[ing] certainty in assessing the applicability of American antitrust law to international business transactions and proposed transactions."9

A third objective was to promote international comity by acknowledging and respecting the prerogatives of other nations to establish and apply their own standards for regulating and remediating alleged restraints of trade in their own markets.10

Congress believed that respecting such foreign sovereign regulatory prerogatives would ultimately best serve U.S. interests by "encourage[ing] our trading partners to take more effective steps to protect competition in their markets."11

Applying state antitrust laws to regulate foreign trade or commerce excluded from federal antitrust jurisdiction by the FTAIA arguably would frustrate every one of these objectives.

American exporters and other businesses engaged in foreign trade or commerce could have no confidence that restraints exempted from federal antitrust attack would not be subject to alternative antitrust attack under the laws of one or more U.S. states. Businesses, therefore, would be deterred from entering into arrangements that Congress intended to enable.

Likewise, ambiguity in the "standard to be employed" for assessing the extraterritorial application of "American antitrust law" would not only persist, but would be multiplied fifty times.

And the imposition of as many as 50 states' antitrust laws on foreign trade or commerce clearly would negate the federal objectives of international comity and respect for foreign regulation of foreign markets.

At every level then, the application of state antitrust laws to foreign trade or commerce exempted by the FTAIA from federal antitrust regulation would "stand[] as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress" in enacting the FTAIA.12

Plaintiffs likely will counter these preemption arguments by pointing out that there is a presumption against preemption and that Congress did not expressly overrule any state antitrust law when enacting the FTAIA.

True, Congress did not address the reach of state antitrust laws, one way or the other, when it enacted the FTAIA. However, the Sherman Act has always extended to "commerce with foreign nations,"13 and was subject to a large body of pre-FTAIA case law addressing the limitations on its extraterritorial reach.14

By contrast, state antitrust laws such as California's Cartwright Act do not expressly reference foreign commerce and have no comparable history of being applied to it.

Congress, therefore, had no cause to be concerned that states would attempt to apply state antitrust laws to foreign trade or commerce exempted from federal regulation by the FTAIA.

Even if there had been such a concern, Congress would have been amply justified in anticipating that the doctrine of implied obstacle preemption — well established when the FTAIA was enacted in 198215 — would resolve any conflict.16

Take California as a specific example. There is a "strong presumption" against preemption, particularly in fields that have been the subject of California's "historic police powers."17 Antitrust plaintiffs would argue that California's "historic police powers" include the authority to regulate competition in California.

On the other hand, the U.S. Supreme Court has consistently held that the power of states to regulate commercial activity outside their borders is necessarily circumscribed.18 That principle applies a fortiori when states attempt to regulate foreign trade or commerce.19

Even in cases involving traditional regulation of conduct within state borders, the California Supreme Court has declined to apply a presumption against preemption where the regulation in question also implicates foreign affairs.20

When the area of regulation encompasses not only foreign trade and commerce but also international relations — that is to say, areas in which federal rather than state interests traditionally predominate — the case for preemption is even stronger.21

Extending the foreign extraterritorial reach of state antitrust laws beyond the limits of the Sherman Act would infringe not only the Supremacy Clause but several additional constitutional provisions establishing federal primacy in the areas of foreign trade, foreign commerce and international relations.22

This allocation of power is intended to ensure that only one entity — the federal government — represents American interests in foreign trade and commerce and foreign affairs.23

In recognition of these principles, courts have repeatedly invalidated state laws that undermine, or threaten to undermine, federal policies and prerogatives in the areas of foreign trade and commerce or foreign affairs.24

These decisions support a conclusion that states cannot constitutionally apply state antitrust laws such as the Cartwright Act to remediate alleged harm from restraints of trade in foreign markets having no direct, substantial and foreseeable anti-competitive effects on trade or commerce in the United States (as would be required for federal antitrust jurisdiction under the FTAIA).

There are policy reasons for this result as well. Claims arising from international cartel conduct or overseas monopolistic behavior arguably seek to apply state antitrust law to decide the legality of foreign conduct (e.g., communications between English and Japanese manufacturers about industry standards, or discussions between Chinese and Korean buyers, or joint ventures in Singapore investing in South America) regardless of whether such conduct was legal when and where it occurred.

Such claims threaten much more than an "incidental or indirect effect" on foreign trade and the internal affairs of foreign countries exercising their sovereign rights to regulate their own markets.25

To assert a state's antitrust law as an all-encompassing international antitrust statute available to police alleged restraints of trade in every country would contravene the federal policy, reflected in the FTAIA, of promoting international comity in this area.26

And allowing one state to apply its antitrust laws to foreign transactions paves the way for every other state to apply its antitrust statutes beyond the limits of the FTAIA.27

Exposure to a thicket of state antitrust regimes would drive foreign companies to avoid doing business that even tangentially affects U.S. commerce.

Finally, such an outcome would conflict with the reported decisions considering this specific issue. One federal court, in In re Intel Corp. Microprocessor Antitrust Litig. ("Intel II"),28 held that California Cartwright Act claims are "limited by the reach of their applicable federal counterparts."29

Intel II analyzed the question as follows:

"Plaintiffs have ... not demonstrated that their state law claims should be applied beyond the boundaries set by the FTAIA ... As the Supreme Court has recognized, '[f]oreign commerce is pre-eminently a matter of national concern,' and therefore, it is important for the Federal Government to speak with a single, unified voice.

"Here, Congress has spoken under the FTAIA with the 'direct, substantial and reasonably foreseeable effects' test, and the Court is persuaded that Congress' intent would be subverted if state antitrust laws were interpreted to reach conduct which the federal law could not."30

The only published California appellate decision on the issue, Amarel v. Connell, similarly holds that the Cartwright Act should not be construed to allow prosecution of extraterritorial antitrust claims that the FTAIA would not.31

The Amarel court observed that "[t]he legislative history of [the FTAIA] discloses it was intended to establish a uniform standard, in the face of conflicting judicial formulations, of the domestic effects necessary to trigger the jurisdiction of American antitrust laws,"32 and that "the proper approach to a preemption analysis is to reconcile 'the operation of both statutory schemes with one another rather than holding one completely ousted.'"33

The court concluded that the plaintiffs' state law antitrust claims were "not preempted" because, as pleaded, the claims did not seek to apply state antitrust laws in a manner inconsistent with the FTAIA.

Rather, they sought damages for anti-competitive practices "alleged to have had an adverse effect on the relevant markets in this state ..."34

According to the court:

"So long as the anticompetitive conduct in question has a direct, substantial and reasonably foreseeable effect within the state, prosecution of the conduct under state law is not precluded."35

In sum, there are strong reasons for a state court evaluating a state law antitrust claim involving foreign trade or commerce to limit the reach of that state law co-extensively with the reach of the Sherman Act as defined by the FTAIA.

To do otherwise contravenes constitutional clauses, rules of statutory construction and federal policies.

## Adv CP

### 2AC

#### Only antitrust can remedy DOJ overstep in Qualcomm because of standing and new SSO incentives

Shapiro 18 [Carl Shapiro is the Transamerica Professor of Business Strategy Emeritus at the Haas School of Business, University of California at Berkeley (go bears), Mark A. † Lemley is the William H. Neukom Professor at Stanford Law School and a partner at Durie Tangri LLP, "THE ROLE OF ANTITRUST IN PREVENTING PATENT HOLDUP", 2018, https://faculty.haas.berkeley.edu/shapiro/patentholdup.pdf]

The FTC’s case against Qualcomm provides a good example of why antitrust is needed. In that case, the District Court found that Qualcomm had breached its FRAND commitment and used its monopoly power over modem chips to pressure its customers (Original Equipment Manufacturers, or “OEMs”) to pay a royalty surcharge for Qualcomm’s SEPs on top of the reasonable royalty rates that Qualcomm would otherwise have been able to obtain. Qualcomm imposed this surcharge when Qualcomm’s customers purchased modem chips from Qualcomm’s rivals.135 The District Court correctly found that Qualcomm’s royalty surcharge acted like a tax when Qualcomm’s customers purchased modem chips from Qualcomm’s rivals.136 Based on this reasoning, the District Court correctly found that Qualcomm’s “no-license/no-chips” policy harmed competition by raising rivals’ costs and thereby excluding them, and that this same conduct also harmed Qualcomm’s customers.137 The Ninth Circuit reversed, making basic errors of both economics and law.

138 On the economics, the Ninth Circuit mistakenly concluded that “Qualcomm’s royalties are ‘chip-supplier neutral’ because Qualcomm collects them from all OEMs that license its patents, not just ‘rival’s customers.’”139 This is flatly incorrect, because the royalty surcharge reduces the gains from trade between an OEM and a rival modem-chip supplier but does not reduce the gains from trade between the OEM and Qualcomm.140 Based on this error, the Ninth Circuit states incorrectly: “The FTC identifies no such harm to competition.”141

On the law, the Ninth Circuit rejects the well-established principle that harming customers can be a way of harming competition: “[T]he primary harms the district court identified here were to the OEMs who agree to pay Qualcomm’s royalty rates—that is, Qualcomm’s customers, not its competitors. These harms were thus located outside the ‘areas of effective competition’—the markets for CDMA and premium LTE modem chips.”142 The notion that harms to customers in the relevant market are outside the scope of the antitrust laws is simply bizarre.

In any event, as noted above, the District Court also found harm to Qualcomm’s rivals in both of the relevant markets it identified. The Ninth Circuit further erred by stating that “the district court’s ‘anticompetitive surcharge’ theory fails to state a cogent theory of anticompetitive harm.”143 The Ninth Circuit’s logic at this point assumes that Qualcomm’s royalties reflect the value of its SEPs, but that is directly contrary to the District Court’s finding that Qualcomm used its monopoly over modem chips to obtain a royalty surcharge, above and beyond the royalties Qualcomm could obtain based on its SEPs.144 One cannot dismiss findings regarding the effects of a royalty surcharge by assuming away that very surcharge. Hopefully the Supreme Court will correct these blatant errors.

Qualcomm’s use of its separate monopoly power over modem chips to evade its FRAND commitment couldn’t be remedied in contract, making antitrust enforcement a necessity for reasons beyond simply enforcing the FRAND deal.145 In the standard-setting context, if a SEP owner breaches its FRAND commitment and is thereby able to charge unreasonably high royalties to device manufacturers, those royalties are likely to be passed through in large part to final consumers. Antitrust enforcement can protect consumers from these overcharges.146

But to the extent that antitrust can step back in some settings, that is only possible because the market participants have recognized and responded effectively to the patent holdup problem by requiring reasonable licensing terms, and because the courts have enforced that requirement in contract or patent law. The second prong of the Antitrust Division’s attack on FRAND commitments therefore undermines whatever merit there might be to the first prong. While on the one hand Delrahim says that we don’t need antitrust because contract and equity will solve the patent holdup problem, on the other hand he is advocating policies that make it harder for contract and patent law to solve that very problem. Threatening SSOs with liability—maybe even per se liability—for trying to stop SEP holdup undermines the very contractual solution on which Delrahim purports to rely. So too do Delrahim’s periodic claims that holdup is a good thing, or at least something we should accept,147 his incorrect claim that patent holdout is a bigger problem than patent holdup,148 and his advocacy for undoing or avoiding eBay and giving a patent owner the right to an automatic injunction.149 Indeed, under Delrahim, the Antitrust Division evidently objects even to voluntary commitments by patent owners not to seek an injunction as part of the standard-setting process.150 Ironically, this assault on SSOs and FRAND policies may actually necessitate more antitrust intervention in standard-setting. If the DOJ encourages companies like Qualcomm to ignore their FRAND commitments, and if the DOJ discourages SSOs from trying to solve the SEP holdup problem, or impedes their efforts to do so, antitrust may ultimately have to step in to protect a functioning market from SEP holdup.

#### Vague FRAND commitments make private enforcement fail

Morton 16 [Fiona Scott Morton, Theodore Nierenberg Professor at Yale School of Management. Carl Shapiro, Former Director of the Institute of Business and Economic Research at UC Berkeley, Professor of the Graduate School at the Haas School of Business and the Department of Economics at the University of California at Berkeley. “Patent Assertions: Are We Any Closer to Aligning Reward to Contribution?”. 2016. https://www.journals.uchicago.edu/doi/full/10.1086/684987#\_i22]

The root cause of many problems in the SEP market described in the following is this vague nature of the FRAND commitments. If the FRAND commitment contained more detail on what actions and rights were permitted or forbidden, the upper range of demands would shrink, thereby making it more difficult for a patent holder to engage in holdup.75 However, SSOs operate by consensus and typically have at least some members who profit from the status quo. Those members can use due process within the organization to slow or block reform. Tactics include filibustering discussions and votes, requiring subcommittees to engage in extensive study, and organizing or purchasing allies to vote against reform. Dysfunction of FRAND enforcement has been noted by policymakers for many years. In January 2013, the US Department of Justice (DOJ) and the US PTO issued a joint policy statement regarding SEPs.76 The National Research Council recently released a detailed study of the IPRs of a number of SSOs, including a series of recommendations for SSO and government policies.77

#### “Antitrust laws” consider competition.

William D. Rohlf Jr. 11, Professor of Economics at Drury University, “Workbook for Introduction to Economic Reasoning: Solutions,” Chegg, 2011, <https://www.chegg.com/homework-help/workbook-for-introduction-to-economic-reasoning-8th-edition-chapter-8-problem-9mc-solution-9780131368576>

(1) Option (a): Antitrust enforcement promotes competition and industry regulation does not, is the primary difference between antitrust enforcement and industry regulation. Antitrust laws ban price fixing, tying contracts and mergers to promote competition. The basic assumption of the industry regulation is that certain industries should not be made competitive.

#### Core is a basic part.

Merriam-Webster ND, Publishing Company, “core noun (1), often attributive,” https://www.merriam-webster.com/dictionary/core

2a: a basic, essential, or enduring part (as of an individual, a class, or an entity)

#### Government R&D can’t solve growth or innovation

Terence Kealey 21. Professor of clinical biochemistry at the University of Buckingham. "Federal Science Funding Won't Accomplish Anything the Private Sector Can't Do Better". Cato Institute. 6-16-2021. https://www.cato.org/commentary/federal-science-funding-wont-accomplish-anything-private-sector-cant-do-better

A bipartisan group led by Senate Majority Leader Chuck Schumer (D-N.Y.) wants to counter China with legislation to dramatically increase government funding of pure science (science that is mainly concerned with theory rather than practical applications). They call their bill the U.S. Innovation and Competition Act. But if they really want to spur innovation and competition, they should be trying to slash science subsidies, not increase them.

The most potent criticisms of the government funding of science have come from government agencies themselves. The first came in 1969 when the Office of the Director of Defense Research and Engineering analyzed 700 research “events” that had led to the development of 20 weapons systems—finding that only two of those events were in pure science.

Then the Congressional Budget Office (in both 1991 and 1998) and the Bureau of Labor Statistics (2007) reviewed the entire academic literature, finding that study after study showed that the research projects that governments funded had failed, on average, to generate profits: in contrast, the research projects that the private sector funded were, overall, highly profitable.

Finally, in 2003 the Organisation of Economic Cooperation and Development, on studying the growth rates of the 21 leading world economies between 1971 and 1998, found that whereas levels of privately funded R&D correlated strongly with national rates of economic growth, there was no positive impact on GDP per capita from publicly‐​funded research and development.

Government funding of science isn’t just ineffective; it crowds out private sector success. When the government subsidizes a company’s science, or when the government pays for a research program, that company or that program will benefit. But the economy at large will suffer, because scientists have been pulled out of the projects the market was trying to fund.

Many view government funding of science as a foregone conclusion. But while the federal government has long funded so‐​called “mission research,” such as the Coast Survey (1807), it didn’t start to fund pure science until 1950, when it established the National Science Foundation (NSF).

The blueprint for the NSF was provided by American engineer Vannevar Bush. In his “linear” or “pipeline” model, he proposed there were both military and market failures in pure science: Only if the government funded pure science would U.S. technology flourish. In the ensuing years, much federally funded research has proven him wrong.

This is a tough story to propagate because the vested interests are aligned. The universities and the scientists lobby for governments to give them money on their own terms; industry lobbies for subsidies; and governments enjoy distributing research money, as the Medicis once did to Galileo. But the data show that these schemes will not benefit the economy.

Advocates for government funding of science will point to the many good things it has helped produce, including the internet. Vast funds for research will indeed yield good things, but the government studies cited above show that the costs of that research merely equal the benefits. In stark contrast, the costs of private research are dwarfed by their benefits. The plural of anecdote is not data; and if we are to get policy right, we should look to systematic cost‐​benefit studies, not anecdotes.

After the Soviets launched Sputnik in 1957, the federal government hugely increased its funding of research. Yet rates of growth in U.S. GDP per capita did not rise, and rates of productivity growth actually fell. That implies that government funding of research crowded out more useful work

## Biz Con

### 2AC – Top

#### Link thumped – a. SEP cases coming that are perceived

Angela Morris 9/17, litigation reporter at American Lawyer Media, reports on cases pending in the federal circuit, 9/17/2021, “The FTC creates a potential new US headache for SEP owners,” https://www.iam-media.com/frandseps/the-ftc-creates-potential-new-us-headache-sep-owners

SEP owners that may already be wary of potential Biden Administration regulatory changes now have a new threat to keep them up at night.

Over the summer the Federal Trade Commission [announced an expanded view](https://www.jdsupra.com/legalnews/the-ftc-expands-section-5-enforcement-7020931/) of its standalone enforcement authority to curb anti-competitive misconduct; and [now the agency has made it clear](https://www.ftc.gov/news-events/press-releases/2021/09/ftc-streamlines-investigations-in-eight-enforcement-areas) that priority targets include “abuse of intellectual property” and “monopolistic practices”.

The agency’s description of the “anticompetitive and deceptive conduct” it seeks to curtail in the technology sector most likely will encompass alleged misconduct by standards essential patent (SEP) owners and their commitments to licensing on FRAND terms, according to IP and antitrust attorney [Tim Syrett](https://www.wilmerhale.com/en/people/timothy-syrett).

“The FTC has previously conducted two investigations where it found that SEP holders seeking injunctions against licensees was anti-competitive and presented a threat to innovation,” Syrett, who is a partner in Wilmer Hale in Washington DC, explains via email. “That may be an area where the FTC wants to continue to devote resources and is certainly an area where there can be harm to competition because of the hold-up power of SEPs.”

Wilmer Hale has represented Apple in high-profile disputes with Samsung, Nokia and Qualcomm, as well as other Big Tech companies in litigations that concern the intersection of patents and anti-trust.

Syrett adds that investment-backed patent assertion entities and patent aggregation organisations may also have reason to fear ITC investigations.

“Investment-backed patent assertion entities can obscure information about who actually owns or has an interest in patents that can harm both licensing and litigation,” says Syrett. “Further, we have seen a concerning rise of patent assertions where the incentives of investors to obtain outsized returns from patents trump any reasonable valuation of the patents’ worth, which can harm competition in the licensing of patents.”

Many in US patent circles may disagree with Syrett's claims about hold-up and PAEs, but the concern will be that they  represent opinion inside the FTC.

The commission has indicated that it will investigate potential abuses of IP rights that create anti-competitive and deceptive conduct, identifying the pharmaceutical, technology and gasoline refining industries by name. Another stated FTC aim is to target alleged abuses of market power that stop entrepreneurs from competing with Big Tech.

These two resolutions were among a group of eight that a divided commission passed this month on a 3-2 vote, as the agency seeks to handle increased workload from high merger filings. Both resolutions, effective for 10 years, direct the agency to use its compulsory processes to obtain documents and testimony through either demands or subpoenas to investigate allegations that would be a violation of Section 5 of the FTC Act.

Section 5 prohibits business conduct that amounts to an unfair method of competition that impacts commerce. Historically, that has meant a violation of federal antitrust laws like the Sherman Antitrust Act or the Clayton Act. However, over the summer, the FTC issued an expanded interpretation of its Section 5 authority that opened room for the agency to use its standalone authority to bring Section 5 enforcements.

The “abuse of intellectual property” resolution would allow FTC staff quickly to conduct investigations into IP rights as a source of anti-competitive and deceptive conduct in the pharmaceutical, technology and gasoline refining industries, said the commission statement that announced the resolutions on 14 September.

[According to the resolution](https://www.ftc.gov/system/files/attachments/press-releases/ftc-streamlines-consumer-protection-competition-investigations-eight-key-enforcement-areas-enable/omnibus_resolutions_p859900.pdf), the agency plans to investigate people, partners or corporations that engage in “unfair, deceptive, anticompetitive, collusive, coercive, predatory, exploitative or exclusionary acts or practices”. The FTC will determine what action to take or remedy to grant, including injunctive or monetary relief that is in the public interest.

Another resolution on “monopolistic practices” addresses bipartisan concerns about market power abuses by tech companies and other large businesses, said the statement. It added that the resolution allows FTC staff to expeditiously investigate dominant players’ abuses that stop other businesses and entrepreneurs from competing – especially in digital markets.

The vote on the resolutions split the commission, with [chair Lina Khan](https://www.ftc.gov/system/files/documents/public_statements/1596260/p859900omnibuslmkrksconcur.pdf) and commissioners [Rohit Chopra](https://www.ftc.gov/system/files/documents/public_statements/1596280/p859900rcomnibusstmtomnibusmilitary.pdf) and Rebecca Kelly Slaughter in favour, and commissioners [Noah Joshua Phillips and Christine S Wilson](https://www.ftc.gov/public-statements/2021/09/dissenting-statement-commissioners-noah-joshua-phillips-christine-s-wilson) opposed.

Syrett says he can’t predict if the agency’s announcement is a prelude to more *FTC v Qualcomm* style investigations, but he does view it as another signal that the Biden Administration takes a different approach to SEP and FRAND issues compared with its predecessor. It goes hand-in-glove with [the president’s executive order in July](https://www.iam-media.com/frandseps/white-house-executive-order-seps-frand-europe) telling the attorney general and secretary of commerce to reconsider a 2019 statement that downplayed the risk of SEPs.

“The prior administration took a decidedly pro-patent holder view when it came to considering harm to competition from SEPs,” says Syrett. “The Biden Administration has shown that it’s willing to return to the consensus view that’s existed across multiple administrations, both Republican and Democratic, that SEPs pose a significant risk of holdup that can harm competition, innovation and consumers.”

#### b. And broader antitrust

Kari Paul 21, technology reporter at Guardian US, “‘They should be worried’: will Lina Khan take down big tech?,” Guardian, 8-1-2021, https://www.theguardian.com/us-news/2021/aug/14/lina-khan-big-tech-ftc-antitrust

Lina Khan has some of the biggest companies in the world shaking in their boots.

The 32-year-old antitrust scholar and law professor in June became the youngest person in history and the most progressive in more than a decade to be appointed as chair of the Federal Trade Commission (FTC).

Khan’s appointment places her at the helm of the federal agency charged with enforcing antitrust law just as it is poised to tackle the giants of the technology industry after years of unchecked power. And it’s clear that big tech isn’t happy about it.

Within weeks of Khan’s appointment, both Facebook and Amazon requested that Khan be recused from the FTC’s antitrust investigations into their companies, arguing that her intense criticism of them in the past meant she would “not be a neutral and impartial evaluator” of antitrust issues.

Khan has forcefully argued for the need to rein in powerful firms like Amazon, Facebook, Apple and Google, developing an innovative antitrust argument that has revolutionized the way we think about regulating monopolies.

“She understands how these companies are harming workers, innovation and ultimately democracy and is committed to taking them head on,” said Stacy Mitchell, co-director of Institute for Local Self-Reliance, an antimonopoly advocacy organization.

“This is a gamechanger.”

‘A meteoric rise’

Before Khan took it on, antitrust law enforcement in the US had atrophied. For decades, it had functioned under the “consumer welfare standard”, which meant that the government would only take action against a company for anti-competitive practices if consumers were hurt by increased prices.

But by the time Khan was a student at Williams and then Yale Law School, tech behemoths had built de facto monopolies by giving away their products for free or at such low prices that no one else could compete.

In the early years of the tech boom it was widely assumed that the industry would essentially regulate itself, according to Rebecca Allensworth, a professor of antitrust law at Vanderbilt University. That Yahoo’s popularity gave way to Google and Myspace to Facebook appeared to be proof that “competition in tech was intensive without any government involvement”, she said. “But we have seen how that has really changed, as has our understanding of how these companies can abuse the market.”

Slipping through the cracks of these old antitrust standards, tech companies amassed unchecked power, acquiring competitors and scooping up billions of customers. In 2020, Apple became the first American company to be valued at $2tn. That same year, Amazon eclipsed $1tn, joining Microsoft, at $1.6tn, and Google parent Alphabet at $1tn.

In her now-famous 2017 Yale Law Journal article, Khan argued that the rise of these mega companies proved that modern American antitrust law was broken, and that the traditional yardsticks by which regulators determine monopolies need to be re-examined for the digital age.

Keeping prices low has allowed Amazon to amass a large share of the market, giving it a disproportionate impact on the economy, stifling competition and further perpetuating monopoly, she argued.

“The long-term interests of consumers include product quality, variety and innovation – factors best promoted through both a robust competitive process and open markets,” she wrote.

She also investigated mergers and examined the impact the resulting tech monopolies have on product quality, suppliers and company conduct. Even if these companies’ practices resulted in some benefits for consumers, they were harmful to markets and democracy at large, she said.

The immediate impact of her thesis was undeniable, with the New York Times announcing Khan had “singlehandedly reframed decades of monopoly law”. Politico called her “a leader of a new school of antitrust thought”. Christopher Leslie, a professor of antitrust law at University of California, Irvine, characterized Khan’s rise in recent years as “meteoric”.

“It’s unprecedented to have somebody ascend to such an important leadership role in antitrust enforcement so soon after graduating from law school,” he said. “But it’s also unprecedented to have somebody make such a significant impact on antitrust public policy debates so quickly after graduating.”

Big tech in the hot seat

In 2019, Khan brought her new approach to antitrust to Congress, serving as counsel to the US House judiciary committee’s subcommittee on antitrust, commercial, and administrative law. Spearheading the committee’s investigation into digital markets, she played a large role in the publication of its landmark report: a 451-page treatise on how companies including Google and Amazon abuse their market power for their own benefit.

Khan also served as legal director at the political advocacy group Open Markets Institute and taught antimonopoly law at Columbia until her appointment to the FTC in 2021.

Khan’s appointment marked a break from the “revolving door” between the FTC and the private sector, in which people with years of experience defending companies in Silicon Valley become regulators. Her new role also comes at a time when reining in big tech is one of the only issues that unites a deeply divided Congress.

The Massachusetts senator Elizabeth Warren said Khan’s leadership of the FTC was “a huge opportunity to make big, structural change” to fight monopolies and Senator Amy Klobuchar praised Khan as “a pioneer in competition policy” who “will bring a critical perspective to the FTC”. The Republican Ted Cruz told Khan he “looked forward” to working with her on these issues.

Khan has her critics. The former Republican senator Orrin Hatch has condemned her thesis as “hipster antitrust”. Mike Lee of Utah said she “lacks the experience necessary” for the FTC and that her views on US antitrust laws were “wildly out of step with a prudent approach to the law”.

But her appointment coincides with a growing drive among lawmakers to take on the major tech companies, Allensworth said. “Politicians, small businesses and the academic establishment are clamoring for it,” she added.

Shortly after naming Khan as chair, Joe Biden signed an executive order calling on federal regulators to prioritize action promoting competition in the American economy – including in the tech space. “Let me be very clear: capitalism without competition isn’t capitalism. It’s exploitation,” he said regarding the order, which contained 72 initiatives to limit corporate power.

Biden asked the FTC to better vet mergers and acquisitions and to establish rules on surveillance. He also called for easing of restrictions on repairing tech devices and data collection on consumers.

‘A different set of rules’

In her first hearing as chair in July, Khan indicated that she was ready to get started, saying the US needs “a different set of rules”.

She cited bad mergers – in the past she had criticized Facebook’s acquisitions of Instagram, Giphy and WhatsApp as anti-competitive – as potentially fueling large tech monopolies: “In hindsight there’s a growing sense that some of those merger reviews were a missed opportunity.”

One of Khan’s first tasks as chair is likely to be rewriting an FTC antitrust complaint against Facebook that was dismissed in June after the agency failed to demonstrate that the tech giant maintains a monopoly.

Meanwhile, Apple and others are set to face FTC scrutiny over repair policies that restrict third-party companies from fixing devices. The agency voted unanimously in July to ramp up enforcement of the right to repair.

The attempts by Amazon and Facebook to force Khan’s recusal are signs that big tech won’t go down without a fight. But critics say these efforts amount to intimidation tactics and not much more. Khan does not have any conflicts of interest under federal ethics laws, which typically apply to financial investments or employment history, and the requests are not likely to go far.

This is “a PR move”, said Allensworth. “She has made a lot of very public, extremely influential arguments about exactly how tech suppresses competition and now she’s the chairperson of the largest and most important federal agency to do with competition,” she said.

“They should be worried,” she added.

#### Biz con low and alt causes

AP 9/29 [Associated Press, "Small and Midsize Business Confidence Falls Amid Rising COVID-19 Cases", 9/29/21, https://apnews.com/press-release/pr-newswire/coronavirus-pandemic-business-health-business-confidence-5057bbef8ca984868c78075871d7baf2]

Confidence among small and midsize business (SMB) CEOs fell in the third quarter of 2021, erasing all gains recorded in the first half of the year, according to the latest CEO Confidence Index from Vistage, a CEO coaching and peer advisory organization. The Confidence Index, which measures sentiment on various economic and business topics among SMB leaders, was 97.1, down from 108.8 in Q2, with 40% of CEOs of small and midsize businesses reporting the increase in cases related to the Delta variant has impacted their businesses. In addition, 41% have made changes to their masking policies as a result, but 56% say they will never mandate vaccines for employees.

“The Delta variant, combined with the economic headwinds of inflation, supply chain challenges and talent scarcity has not fully reversed the economic surge that occurred as restrictions lessened; however, it has slowed growth expectations. Small business owners are still trying to navigate how to keep their businesses running while keeping their employees safe,” said Joe Galvin, Vistage’s chief research officer. “Economic growth will continue through the second half of the year, just not at the unsustainable pace of the first half.”

For now, the pandemic continues to impact employment with 67% of leaders saying they are struggling to operate at full capacity given staffing challenges, and 66% reporting they are planning on hiring in the next year. To combat these challenges, businesses are using a variety of incentives: boosting wages (69%), expanding benefits (28%), offering hiring bonuses (27%) and allowing remote working (41%). Current employees are also being offered skill development programs (56%) and increased overtime (26%).

#### Not key to growth

Cameron Bagrie 18, Managing Director of Bagrie Economics, “Business confidence is a hopeless indicator. But that doesn't mean the economy isn't in trouble,” Spinoff, 8-9-2018, https://thespinoff.co.nz/business/09-08-2018/business-confidence-is-bullshit-but-that-doesnt-mean-the-economy-isnt-in-trouble/

The good news is that business confidence is hopeless as an economic indicator. The correlation with economic growth is poor and I largely ignore business confidence readings. Changes in direction can provide some insightful information – whether things are picking up or slowing down, but not the levels.

Businesses tend to be more upbeat regarding general confidence about the economy under a blue flag as opposed to a red one. Business confidence averaged minus 18 between 2000 and 2007. The economy (measured by real gross domestic product) grew on average by more than 3.5% per year. Yep, confidence was negative, but growth was positive. So, we ignore business confidence as an economic indicator. This is nothing new. It’s surprising headline business confidence figures receive so much attention

#### No econ impact

**Walt 20** [Stephen M. Walt is the Robert and Renée Belfer professor of international relations at Harvard University. “Will a Global Depression Trigger Another World War?”, May 13th, https://foreignpolicy.com/2020/05/13/coronavirus-pandemic-depression-economy-world-war/]

On balance, however, I do not think that even the extraordinary economic conditions we are witnessing today are going to have much impact on the likelihood of war. Why? First of all, if depressions were a powerful cause of war, there would be a lot more of the latter. To take one example, the United States has suffered 40 or more recessions since the country was founded, yet it has fought perhaps 20 interstate wars, most of them unrelated to the state of the economy. To paraphrase the economist Paul Samuelson’s famous quip about the stock market, if recessions were a powerful cause of war, they would have predicted “nine out of the last five (or fewer).”

Second, states do not start wars unless they believe they will win a quick and relatively cheap victory. As John Mearsheimer showed in his classic book Conventional Deterrence, national leaders avoid war when they are convinced it will be long, bloody, costly, and uncertain. To choose war, political leaders have to convince themselves they can either win a quick, cheap, and decisive victory or achieve some limited objective at low cost. Europe went to war in 1914 with each side believing it would win a rapid and easy victory, and Nazi Germany developed the strategy of blitzkrieg in order to subdue its foes as quickly and cheaply as possible. Iraq attacked Iran in 1980 because Saddam believed the Islamic Republic was in disarray and would be easy to defeat, and George W. Bush invaded Iraq in 2003 convinced the war would be short, successful, and pay for itself.

The fact that each of these leaders miscalculated badly does not alter the main point: No matter what a country’s economic condition might be, its leaders will not go to war unless they think they can do so quickly, cheaply, and with a reasonable probability of success.

Third, and most important, the primary motivation for most wars is the desire for security, not economic gain. For this reason, the odds of war increase when states believe the long-term balance of power may be shifting against them, when they are convinced that adversaries are unalterably hostile and cannot be accommodated, and when they are confident they can reverse the unfavorable trends and establish a secure position if they act now. The historian A.J.P. Taylor once observed that “every war between Great Powers [between 1848 and 1918] … started as a preventive war, not as a war of conquest,” and that remains true of most wars fought since then.

The bottom line: Economic conditions (i.e., a depression) may affect the broader political environment in which decisions for war or peace are made, but they are only one factor among many and rarely the most significant. Even if the COVID-19 pandemic has large, lasting, and negative effects on the world economy—as seems quite likely—it is not likely to affect the probability of war very much, especially in the short term.

## Politics

### 2AC—Politics—BBB

#### Manchin will punt it to next year AND thumpers.

Hans Nichols 11/10, Political Reporter for Axios, former Pentagon Correspondent for NBC News, Former International and White House Correspondent for Bloomberg News, “Manchin may delay Biden social spending plan over inflation,” Axios, 11/10/21, https://www.axios.com/manchin-chill-bbb-6b58cd70-6c07-40f9-af4e-c944a7b3a39d.html

Red-hot inflation data validates the instinct of Sen. Joe Manchin (D-W.Va.) to punt President Biden’s Build Back Better agenda until next year — potentially killing a quick deal on the $1.75 trillion package, people familiar with the matter tell Axios.

Why it matters: The data released Wednesday set the president and White House staff scrambling. Slowing down work on the massive tax-and-spending plan is against the fervent desire of the administration and House progressives.

With a limited number of legislative days left in the year, Manchin is content to focus on the issues that need to be addressed, Axios is told.

They include funding the government, raising the debt ceiling and passing the National Defense Authorization Act.

Manchin, like a group of House moderates, also wants to see a Congressional Budget Office analysis of the true cost of each of Biden’s proposed programs, as well as the tax proposals to fund them.

The big picture: Progressives have long worried that after centrists got their $1.2 trillion bipartisan infrastructure bill, they'd find excuses not to move on the budget reconciliation package.

It includes billions to expand the social safety net and fight climate change, among other Democratic priorities.

Business groups also are stepping up their attacks on the package, warning congressional Democrats about its overall costs, potential effects on inflation and $800 billion in corporate tax increases.

Manchin still hasn't agreed to the specifics of Biden's plan to spend $555 billion to combat climate change.

Senate Majority Leader Chuck Schumer convened a call today with senators who participated in COP26, where they discussed how climate provisions in both bills were well received in Glasgow.

During the call, the senators also strategized about how to get Manchin to agree to Biden's climate provisions — a recognition they have more work to do.

Driving the news: Prices rose 0.9% from last month for an annual inflation rate of 6.2%, according to the Bureau of Labor Statistics.

The president labeled it "worrisome, even though wages are going up."

He told a crowd in Baltimore: "[O]n the good side, we're seeing the highest growth rate in decades, the fastest decrease in unemployment ... since 1950."

White House chief of staff Ron Klain tried to couch Biden's spending plan as a long-term strategy to lower inflation.

"What it does is it makes sure that our federal spending meets the things that families really need: bringing down the cost of child care, bringing down the cost of drugs, bringing down the cost of elder care, bringing down the cost of preschool, cutting taxes for middle-class families," he told CNN's Jake Tapper:

Between the lines: Manchin has been warning about inflation since the summer.

He's argued Congress should take a “strategic pause” on the bigger package until Congress had more time to assess the effects of the nearly $5 trillion COVID stimulus spending in 2020 and earlier this year.

His statements on Wednesday amounted to an I-told-you-so.

“By all accounts, the threat posed by record inflation to the American people is not ‘transitory’ and is instead getting worse,” Manchin said. “From the grocery store to the gas pump, Americans know the inflation tax is real and D.C. can no longer ignore the economic pain Americans feel every day.”

#### It’ll get delayed—CBO

Ryssdal 11/11 [Kai Ryssdal and Richard Cunningham, "Congress’ budget gurus may slow down Biden’s Build Back Better plan", 11/11/21, https://www.marketplace.org/2021/11/11/congress-budget-gurus-may-slow-down-bidens-build-back-better-plan/]

On Friday, Congress passed its bipartisan infrastructure bill. The legislation included funding for classic city infrastructure like roads, bridges and transit and other projects such as nationwide broadband internet and power and water systems. Progressives in Congress are now focused on the Build Back Better Act, legislation that contains President Joe Biden’s plan to expand the social safety net in the U.S.

But right now, the Congressional Budget Office may slow down those plans.

“Marketplace” host Kai Ryssdal spoke to Zach Moller about CBO scoring and its role in the legislative process. Moller is a federal budget policy expert and director of the economic program at Third Way, a center-left think tank in Washington.

The CBO is a nonpartisan federal agency that estimates the economic impact of legislation and provides fiscal analysis of Congress’ proposals. Moller said the office is essentially in charge of figuring out what a policy would cost or how much money a policy can save.

“That means if a bill is 2,000 pages long, they’re going into each section of the bill and figuring out what that particular section is going to cost or what it’s going to save,” Moller said.

The work of the CBO is incredibly detailed. Several times a year, the CBO creates a budget baseline to judge future legislation. The baseline, a 10-year economic forecast, is predicated on how the economy is working at that time, and it includes factors like the tax code, inflation and interest rates. From this baseline, the agency develops scores to estimate a bill’s impact.

“It requires a substantial amount of technical expertise to do what they do,” Moller said. “It requires a lot of time and effort to get the numbers right.”

For the Build Back Better Act, the CBO score is extremely important. Senate Democrats are contemplating passing the bill through the budget reconciliation process, a procedure that enables Congress to pass certain fiscal and budgetary legislation with a simple majority. But this method comes with additional regulations, Moller said.

The “CBO score is vital because the Senate parliamentarian is going to have to weigh in on whether or not individual parts of the bill meet the requirements of this special process that they are using,” Moller said.

The CBO must share its score with the Senate before the bill can be passed. To make matters more complicated, moderate Democrats may not be happy with the price of Biden’s Build Back Better legislation, currently tagged at about $1.75 trillion.

A group of moderate Democrats in the House released a statement committing them to vote for the bill. However, they must receive a CBO score by the week of Nov. 15, they said. But House Budget Chairman John Yarmuth told CNN that a CBO score could take up to two weeks to produce. Some say it might not be ready before Thanksgiving.

Moller said these projections require extremely detailed work, but it’s “superimportant.”

“I think that’s a really essential part of why CBO takes so long,” he said. “Because they’re doing a more detailed look at what’s going on in this legislation than anyone else.”

House Speaker Nancy Pelosi has said the plan is still to pass the bill during the week of Nov. 15, when the House returns from recess. But without the CBO score, it might take longer than expected.

Ev doesn’t say it solves CC anywhere

**Lawmakers will compartmentalize conflict on separate issues**

**Pergram 18** (Chad Pergram, Congressional reporter. “Amid Kavanaugh cacophony, Congress forges bipartisan agreements on key issues”. October 13, 2018. <https://www.foxnews.com/politics/amid-kavanaugh-cacophony-congress-forges-bipartisan-agreements-on-key-issues>)

Step back from the Kavanaugh cacophony. Examine what lawmakers from both parties in both chambers accomplished in September and early October, with virtually zero fanfare. **Amid** the **turmoil**, Congress approved the first revamp of national aviation policy in years. The Senate approved the final version of the legislation 93-6. This came after a staggering six extensions due to bickering and disagreement. Then, Congress approved a sweeping, bipartisan measure to combat opioid abuse. The House okayed the package 393-8. The Senate adopted the measure 98-1. And, there was no government shutdown. The House and Senate came to terms on two bipartisan bills which funded five of the 12 annual spending bills which operate the government. The sides agreed to latch an additional measure to one of the spending plans to fund the remaining seven areas of federal spending through December 7. President Trump briefly threatened to force a government shutdown if lawmakers didn’t include money for his border wall in the plan. But the President ultimately punted that battle until December. Democrats praised Republicans for keeping conservative “poison pill” riders out of the appropriations bills. That decision drew Democratic support for the measures. The Senate approved a bipartisan **water and infrastructure** package. McConnell hailed the **bipartisanship** which descended upon the Senate – **even as the senators fought over Kavanaugh**. Nearly **in the same breath**, McConnell derided boisterous, anti-Kavanaugh protesters outside the Capitol as a “mob.” McConnell insisted this week he needed the Senate to clear a slate of 15 conservative judges to lower courts before he could cut senators loose for the midterm elections. McConnell and Schumer appeared at loggerheads. McConnell’s goal was clear: extract the confirmation of these nominees – or tether to Washington vulnerable Democratic senators from battleground states to keep them off the campaign trail. Schumer knew McConnell would ultimately prevail on the nominees after the midterms. So the New York Democrat accepted McConnell’s ransom, permitting the Senate vote on a slate of nominees on Thursday night. Schumer also extracted a concession from McConnell: send senators home until November 13th. One may wonder how lawmakers can find themselves in an **imbroglio** over a major issue like Kavanaugh – **yet forge major bipartisan accords on other**. Frankly, that’s just politics. Politics always elicits strange bedfellows. Successful lawmakers know they should **compartmentalize their disputes**. The enemy today may be your best ally tomorrow.

#### Aff is bipartisan and popular

Muris 17 [Timothy, Foundation Professor of Law at George Mason University’s Antonin Scalia Law School and Senior Counsel at Sidley Austin LLP. “Bipartisan Patent Reform and Competition Policy”. May 2017. https://www.aei.org/wp-content/uploads/2017/05/Bipartisan-Patent-Reform-and-Competition-Policy.pdf]

Finally, I have outlined how antitrust law can assist contract and patent law in limiting holdup. Under Republicans and Democrats, the antitrust agencies have pursued anticompetitive conduct. Despite disagreement on particular cases and on the underlying theory under which cases should proceed, there is widespread agreement on the importance of the issue and its suitability as an appropriate subject for antitrust enforcement. Further attention to patent holdup in the Trump administration is warranted and would continue the bipartisan focus on this vital issue.

#### Climate models are wrong- we can adapt

* peer-reviewed journal shows IPCC exaggeration
* social cost estimates are overblown
* historical records are wrong- using physically realistic measures proves decreased impact
* climate cost estimates are inflated by neglecting adaptation

Lau 18 [Matthew Lau, contributing writer to Canadians for Affordable Energy, citing peer reviewed studies from journal nature climate change and Journal of Climate, “Climate change data is wildly overestimated”, 8/14, https://torontosun.com/opinion/columnists/guest-column-climate-change-data-is-wildly-over-estimated]

A study last year by Thorsten Mauritsen and Robert Pincus in the journal Nature Climate Change and another one this year by Nicholas Lewis and Judith Curry in the Journal of Climate, produced median estimates suggesting that a doubling in atmospheric carbon dioxide would increase global temperatures by only about half of what Intergovernmental Panel on Climate Change (IPCC) models predict.

Recently, two Heritage Foundation scholars and Canadian economist Ross McKitrick re-estimated the social cost of carbon dioxide emissions using earlier empirical estimates from Lewis and Curry, instead of relying on simulated estimates of the sensitivity of temperature to carbon dioxide concentration in the atmosphere. In one model, the social cost of carbon fell 40-50% and in another the costs dropped a staggering 80%.

In addition to future warming and its associated costs likely being over-predicted by climate models, historical warming might also be less than what most temperature records suggest. That is because some techniques for producing temperature records systematically display more warming than actually occurred.

According to Patrick J. Michaels and Ryan Maue, scientists with the Cato Institute, one of the most reliable temperature data sets is from the Japan Meteorological Office. This record also shows the least amount of warming. “The fact of the matter is,” the Cato researchers write, “that what should be the most physically realistic measure of global average surface temperature is also our coolest.”

Not only is the amount of warming often exaggerated, but climate cost estimates are often inflated by assuming that humans will not adapt to the warmer climate. This assumption makes no sense when we consider how long the warming is supposed to take and how creative our society is when it comes to solving complex problems.

Adding all this up suggests that climate change probably won’t be anywhere near as disastrous as many people imagine. This has profound policy implications – it means that the drastic and expensive tax and regulatory actions taken by governments in the name of saving the climate are increasingly difficult to justify.

# 1AR

### Adv CP

#### Public R&D causes crowd-out and impedes private investment.

Marino et al. 16, \*Marianna Marino and Stephane Lhuillery, ICN Business School, Department of Strategy and Entrepreneurship; \*Pierpaolo Parrotta and [Davide Sala](https://www.sciencedirect.com/science/article/pii/S0048733316300555#!), Aarhus University, Tuborg Research Centre for Globalization and Firms; (June 17th, 2016, “Additionality or crowding-out? An overall evaluation of public R&D subsidy on private R&D expenditure”, https://www.sciencedirect.com/science/article/pii/S0048733316300555)

6. Discussion and conclusions

This paper is an overall evaluation of the public subsidies to R&D, which proposes an assessment of this policy in absence or combination with the R&D tax credit, an equally important policy instrument used to stimulate private R&D investments. Using a dataset of French companies that covers the period 1993–2009, we perform both inter-group and intra-group assessment of the outcome of this policy. The former analysis is directed to investigate a differentiated impact of R&D grants across differently funded firms, and is presented alongside utilization of the categorical matching method. The latter analysis investigates the implications of the current modulation of public intervention for similarly funded firms. Implemented by means of a continuous treatment evaluation method, the intra-group assessment allows us to investigate the likelihood of crowding-in and crowding-out effects within each tercile along the distribution of the public R&D support grant. Both methods are coupled with the DID approach to account for unobserved heterogeneity and results strengthened by a rich dataset featuring comprehensive information on the pre-treatment variables. In addition, exploiting the exogenous variation due to the sharp change in R&D tax [credit policy](https://www.sciencedirect.com/topics/economics-econometrics-and-finance/credit-policy) that occurred in 2004, we compare [treatment effects](https://www.sciencedirect.com/topics/economics-econometrics-and-finance/causality-analysis) on growth of R&D private expenditure between before- and after-reform periods, and therefore we identify the effects of such a policy change introduced by the government.

Our results show that substitution between private and public funds may occur, especially for medium-high levels of public subsidies, and under the regime of R&D tax credit. Recipients of larger doses appear not to outperform or to perform worse than recipients of lower doses or non-recipient firms. Crowding-out seems stronger and more significant in the after-reform period as reported in both the propensity score and exact matching analysis performed by year. In addition, we find evidence of more extensive negative effects for firms employing fewer than 100 employees or operating in low R&D intensive industries. When analyzing the intra-tercile distribution of public funds under R&D tax credit regime, we highlight a considerable reduction in the growth of private R&D expenditure among medium-high subsidy recipients, whereas additionality effects are found for a few top beneficiary companies (above EUR 10 million). In the sample of fully supported recipients, it seems to emerge – on average – that firms receiving subsidies between EUR 145 thousand and 1.8 million exhibit significant lower private contribution with respect to their counterfactual units. Subsidy-only recipients instead show significant substitution of private with public R&D resources for subsidy doses between EUR 20–55 thousand. Interestingly, when dividing the sample in before- and after-reform periods, we find that crowding-out effects seem to persist solely for recipients of subsidies under tax credit incentives after the 2004 reform.

Overall, our findings appear to suggest a substantial re-design of both the modulation and targeting of the public R&D subsidy policy, especially under R&D tax credit regime. Indeed, the substitution effects emerging from the inter-tercile and funded versus unfunded comparisons would motivate a better targeting of the recipient firms, especially among [small and medium size firms](https://www.sciencedirect.com/topics/economics-econometrics-and-finance/sme) and in low R&D intense industries. Concerning the modulation of the public R&D subsidy provision, it appears opportune to move resources from medium-high to top beneficiary recipients to boost the growth of private R&D expenditure and rise the private contribution to R&D in the economy. Furthermore, the distinction between fully funded from subsidy-only recipient firms underlines the importance of accounting for “hidden treatments” that may otherwise affect the policy evaluation and favor misleading implications. In addition, the 2004 reform of R&D tax credit appears to have lowered the effectiveness of public R&D funding. Although this result shed some lights on the effects of the 2004 reform, it also asks for further research to investigate the opportune mix of such R&D policy tools. Finally, it is worth underlining that a potential limitation of our study is due to the fact that we do not observe companies with fewer than 20 employees in the manufacturing industries, a significant proportion of the French firm population.

This overall assessment indicates that an ex-post evaluation of the targets of an R&D policy is desirable, if not necessary in a time of downturns or economic stagnation. In fact, if R&D funding is seen as a valid policy instrument to support companies hit hard by a crisis and facing financial restrictions, it is inevitable that public resources should not be re-directed away from risky and promising research projects toward companies that would likely perform equally well without this funding.

#### Patent law fails because of standing – conceded melamed means its game over because the CP doesn’t establish outside standing

Cary 11 [George Cary, Mark Nelson, Steven Kaiser, Alex Sistla. Cary and Sistla are members of the California and District of Columbia Bars. Mr. Nelson is a member of the New York and District of Columbia Bars. Mr. Kaiser is a member of the New Jersey and District of Columbia Bars. “THE CASE FOR ANTITRUST LAW TO POLICE THE PATENT HOLDUP PROBLEM IN STANDARD SETTING”. Antitrust Law Journal No 3. (2011). https://www.clearygottlieb.com/~/media/organize-archive/cgsh/files/publication-pdfs/the-case-for-antitrust-law-to-police-the-patent-holdup-problem-in-the-standard-setting.pdf]

One final point about patent remedies concerns standing: it is not just the type of harm that matters to antitrust, but whether anyone has a remedy to address it. Antitrust fills the gap left open by patent law by providing a remedy to those “outsiders”—consumers, competitors and others—who lack standing to seek relief under the patent laws. Consider Qualcomm: The use of equitable estoppel there was only available as a defense asserted by the alleged infringer. The elements of the defense discussed above, moreover, require that the infringer either be involved in the SSO process or have a specific basis for claiming that it was affirmatively misled by the patentee. No consumer injured by the wrongful acquisition of monopoly power in this context would meet these criteria, nor would other firms that have been excluded from the market due to the deception at issue. There is no government enforcement agency to protect such plaintiffs, because patent law has no provision for government enforcement intended to protect consumers from harm to competition.

In sum, the limitations of patent law would exclude many of the categories of potential plaintiffs suffering antitrust injury as a result of standard-setting abuse. We conclude that equitable estoppel is unequal to the task of policing monopolization through fraudulent conduct in the standard-setting process.

### DA

#### Biz Con massively down – Supply chain and inflation – these are still impacted EVEN with vaccinations

AP News 11/1 [AP News, “October survey shows growth, but scant confidence in economy”. 11/1/21. https://apnews.com/article/business-economy-business-confidence-b1faa63ec73382488b241f1b023db86f]

But the survey’s business confidence index, which looks ahead six months, failed to budge from 37 recorded in September. That’s the lowest reading the confidence index has reached since March 2020, when the global COVID-19 pandemic began.

The report indicates that the region is adding manufacturing business activity at a positive but somewhat slower pace.

“Almost one-third of supply managers reported that inventory stockpiling has contributed significantly to supply chain bottlenecks,” said Creighton University economist Ernie Goss. who oversees the monthly survey.

Business leaders reported strong job growth, with the employment index rising to 66.1 in October from September’s 56.7. Even so, the region has yet to recover all job losses from the pandemic, Goss said.

Wholesale prices continue to climb, with that index registering 96.5 from September’s 94.9, indicating growing pressure from inflation.

#### Bizcon low---multiple indicators

Marcos ’9/28 [Coral; September 28, 2021; New York Times, “Stocks tumble in worst day since May, as tech shares slide and bond yields climb,” https://www.nytimes.com/2021/09/28/business/stock-market-today.html]

The prospect of the Federal Reserve not reaching as deep into its bottomless pockets is starting to hit home for investors.

The S&P 500 tumbled 2 percent on Tuesday — the worst one-day slide for the benchmark U.S. index since May — as investors faced the expected wind-down of the enormous bond purchases the central bank has made since the start of the pandemic.

“The deep sell-off highlights the extent of the nerves in the markets surrounding the moves of the Fed,” said Fiona Cincotta, senior financial markets analyst at Forex.com.

The coming slowdown of bond purchases is a sign of the Fed’s confidence that the economy is recovering from the upheaval of the pandemic. But, Ms. Cincotta noted, other factors are still making Wall Street wary.

“There’s also a combination of rising energy prices, concerns that inflation could be more entrenched in these elevated levels and the fact that consumer confidence is slowing,” she said.

The tumble extended into the Asian trading day on Wednesday, though investors signaled that confidence might be returning.

Stocks in Japan were down more than 2.6 percent midday. But losses in other Asian markets, like Hong Kong and mainland China, were more moderate. Futures markets were signaling that Wall Street would open modestly higher.

The trigger for Tuesday’s tumble, which cut across sectors, was a rise in the yield on the benchmark 10-year Treasury note. With the Fed preparing to slow its purchases as soon as November, investors have been selling off bonds before demand ebbs. On Tuesday, that pushed the 10-year’s yield up to 1.54 percent, its highest level since June.

Even though the Fed has said it doesn’t plan to increase interest rates for months or years, government bond yields are the basis for borrowing costs across the economy. When bond prices fall, yields rise — a move that can hinder the stock market’s performance because it makes owning bonds more attractive and can discourage riskier investments.

Higher rates would make borrowing more expensive for smaller companies, and the jump in yields was a blow to shares of several high-flying stocks. Etsy, the online craft marketplace, dropped 6 percent, and Shopify fell more than 5 percent. Both companies have soared during the pandemic.

“With tech stocks, you’re betting for a company to have a breakthrough years from now,” said Beth Ann Bovino, the chief U.S. economist at S&P Global. “If interest rates go up today, that value that you receive years from now is discounted.”

The biggest technology stocks — particularly Amazon, Apple, Microsoft, Google and Facebook — have a vast pull on the broader market and helped drag down the S&P 500. Apple fell 2.4 percent and was the best performer of the tech giants. Amazon dropped 2.6 percent while Microsoft, Facebook and Google were down by more than 3.5 percent.

But the declines cut across many sectors. Energy stocks were the exception, rallying after oil prices climbed early in the day. Schlumberger, ConocoPhillips, Halliburton and Exxon Mobil were among the best-performing shares in the S&P 500, though some of their gains faded as oil futures turned lower in the afternoon.

The Delta variant of the virus remains a concern for investors, while persistent supply-chain bottlenecks have affected everything from auto production to school lunches. In Washington, lawmakers remain deeply divided over spending on infrastructure and expanding social programs.

#### Antitrust enforcement is full steam ahead on all fronts---including Europe

Margaret Harding McGill 21, technology reporter at Axios, “Fall antitrust forecast: Biden raises hammer on Big Tech,” Axios, 8-30-2021, https://www.axios.com/antitrust-big-tech-apple-google-amazon-facebook-2e619cf6-2fd9-48be-bc72-0e36cb7fdcfb.html

The antitrust scrutiny of tech giants that began during the Trump era will only intensify this fall as Big Tech critics Lina Khan, Tim Wu and Jonathan Kanter take the lead on competition policy and enforcement in the Biden administration.

Why it matters: Facebook, Google, Amazon and Apple face threats from federal regulators, Congress, state attorneys general and European Union authorities.

The big picture: That's four companies each being challenged from four directions: No wonder the antitrust arena can feel like three-dimensional chess.

As the fall season looms, here's what the game board looks like:

Facebook

The Federal Trade Commission, now led by Khan, renewed its legal effort challenging Facebook's acquisitions of Instagram and WhatsApp in August. The FTC accuses Facebook of buying rivals or using anticompetitive tactics to stymie them in order to squelch competition.

What to watch: Facebook has until Oct. 4 to respond.

The European Commission launched an antitrust investigation of Facebook Marketplace in June over concerns that Facebook's collection of data from advertisers gives it an unfair advantage.

What to watch: The United Kingdom announced a similar investigation in June that also focuses on Facebook's online dating service.

In Congress, the House Judiciary Committee narrowly approved a slate of tech antitrust bills, including one that would force more interoperability and another that would bar big companies from snapping up rivals through acquisitions.

What to watch: Bipartisan companion legislation in the Senate would give these bills some momentum. Sen. Tom Cotton (R-Ark.) said in July he intends to introduce a bill that would curb mergers among big tech companies.

Amazon

The FTC has been investigating Amazon's business practices since the Trump administration and is also digging into the e-commerce giant's plan to buy Hollywood studio MGM.

What to watch: Amazon wants Khan to recuse herself from FTC's Amazon cases, given her previous advocacy of action against the company.

The European Commission accused Amazon last November of violating antitrust rules by harnessing data it collects from third-party sellers to shape the products it offers that compete with those merchants.

What to watch: The commission also opened a separate investigation into how Amazon selects which products get the coveted "Buy Box" label. But a Financial Times story in March suggested that case has been an uphill climb.

In Congress, Amazon faces the potential for drastic changes to its business model through the House antitrust bills that would bar it from both operating its online marketplaces and selling goods on them.

What to watch: Amazon is warning sellers that they could bear the brunt of the cost if such legislation is enacted — and hoping those sellers will call their representatives.

Google

The Justice Department and several state attorneys general filed multiple antitrust lawsuits against Google last year, with the DOJ accusing Google of an illegal monopoly in online search and search advertising.

What to watch: The judge in DOJ's case indicated it likely won't go to trial until 2023. President Joe Biden nominated Jonathan Kanter, an antitrust attorney who has battled Google on behalf of its tech foes, to lead the antitrust division of the DOJ, though he has not yet been confirmed by the Senate.

In Congress, Google faces multiple legislative threats, from the House antitrust bills as well as legislation in both the House and the Senate that would curb its power over its Google Play Store.

What to watch: State attorneys general also sued Google over how it operates its app store.

The European Commission opened its own investigation in June into Google's power in the online advertising ecosystem.

What to watch: Previous European antitrust investigations into Google have led to billions of dollars in fines.

Apple

In Congress, Apple is facing proposed laws in both House and Senate that would limit its control over how it runs its App Store.

What to watch: Apple recently offered some concessions on its App Store policies to settle a class-action lawsuit — but not enough to satisfy those who back these bills.

The European Commission, acting on a complaint by Spotify, accused Apple in April of violating antitrust laws by requiring rival music streamers to use its in-app payment system and follow other rules.

What to watch: The commission opened a separate investigation in June to more broadly review Apple's rules for app developers.

The Justice Department is reportedly also investigating Apple for anticompetitive practices, although that probe has led to no charges so far.

#### Link turn outweighs the link

Bauer et al. 17, \*Matthias Bauer is Senior Economist at ECIPE; \*Fredrik Erixon is a Swedish economist and writer. He has been the Director of the European Centre for International Political Economy (ECIPE) ever since its start in 2006; (October 2017, “Standard Essential Patents and the Quest for Faster Diffusion of Technology”, https://ecipe.org/publications/standard-essential-patents/)

It is easy to take a pessimistic view about whether the system will break. If the current trend continues, the system is likely to break at some point for the simple reason that companies will not trust it anymore. The series of legal disputes witnessed over the past years – sometimes referred to as the “smartphone patent wars” – has been fodder for a pessimistic reading of “the two tales of SEPs”. While it is common in the business world that disputes over patents and licenses are settled in courts, various SEP disputes have revealed problematic aspects of the SEP market that are different from those disputes that follow the normal stream of business and contracts. Often, the SEP disputes are less concerned about the rights and boundaries of patents, and more about antitrust limits to market behavior: they concern market abusive practices and restrictions to competition as much as they are about intellectual property.

If the SEP system actually does break at some point, the consequences would be felt throughout the economy. SEPs have been a critical part of the ICT revolution. SEPs have allowed for the fast rates of innovation diffusion that the world has witnessed over the past quarter of a century. All the computer and Internet related products and services that people are now dependent upon for their private and professional lives are intricate webs of intellectual property. As many as 250,000 patents can be used to claim ownership of some technical specification or design element in a single smartphone (NYT 2012). A laptop, suggests one calculation, implements more than 250 interoperability standards (Biddle et al. 2010), and the number of SEP holders for 3G and 4G standards grew from 2 in 1994 to 130 in 2013 while the number of SEPs rose from fewer than 150 in 1994 to more than 150,000 in 2013 (Galetovic and Gupta 2016). The standardization-body ETSI has registered more than 150,000 declarations of SEPs from companies, and ETSI is just one of many bodies in the world of ICT standardization. For the 3G standard, the same body has about 24,000 patents that have been declared essential. Now, with the economy yet again on the threshold of big technological change, a trusted and credible system for creators and users of technology to standardize proprietary technology would be a boon for innovation, interoperability and – ultimately – the consumers.

And there are reasons for optimism. Although many of the problems in the SEP regimes need to be addressed, the numbers above indicate that the SEP system is in fact attractive to patent holders and SEP implementers. It is easy to see why: neither holders nor implementers are presented with alternative options that on the face of it would be far more profitable for them. In other words, there simply would not be as many patents declared as essential if both creators and users of technology believed the SEP system worked to their disadvantage or was grossly unfair. While the reality for some companies may be that legal disputes and unpredictability prompt them to find other ways than SEPs to get access to key technologies for their products, it remains the case that most stakeholders have strong economic incentives to maintain a balanced SEP system that is trusted.

First, standard essential patents are an asset for creators of technology because, by becoming essential to a standard, their volumes of sales for technologies that users value rise significantly. As many holders want to raise more revenues for their SEPs and – ideally – have the freedom to contract with buyers on their terms, they can expand their customer base when they agree to sell patented technology in accordance with a set of rules that are designed to prevent SEP holders exploiting the weakness of a customer that has grown dependent on having access to their technology.

Second, SEPs are hugely beneficial also to those that buy the licenses – the implementers or users. Through the SEP system, they can access technologies that are interoperable and work with different products and functionalities – and they can do it under conditions that, if history is a guide, in most cases give them stable and predictable terms of contract. As a consequence, both creators and users can focus on their competitive advantages and profit on the economies of scale and specialization. Downstream firms do not need to develop their own upstream technology and upstream firms do not need to package their technologies in end-customer products in order to make their products valuable.

Third, standard-setting organisations (SSOs) also have a big stake in an SEP system that works well – and, like creators and users of technology, they would stand to lose significantly if the SEP system were to collapse.

Lastly, the biggest beneficiaries are individual consumers – those who buy the end products using FRAND-conditioned SEPs. The advent of SEPs and the rules represented by FRAND have enabled a development of fast technology creation and contributed to the rapid diffusion in ICT goods and ICT-based services. The SEP system has also allowed for new competition, both between existing technologies and brands, and from new ones that have stepped into the market with the ambition to disrupt it, again to the benefit of the consumer. It is difficult to imagine that the ICT and digital development would have been as fast as it has been if SEPs had not been a central feature of the market.

The changing fortunes of companies operating in the cellular and smartphone market would not have been possible if there had not been an SEP system that supported competition. Now that the world economy is on the doorstep of new innovations that are dependent on a great number of input technologies – e.g. the Internet-of-Things, transport connectivity and intelligent vehicles – it is crucially important for the consumer that a balanced and functioning SEP system is maintained and that actors in the system converge towards it – which would ultimately meet their economic interests.