# 1AC — SEP’s

## 1AC

### 1AC---FRAND ADV

#### Advantage 1 is FRAND:

#### Standards-Setting Organizations (SSO’s) are industry members who jointly establish standards for information tech defined by the adoption of standard-essential patents (SEP’s), which are licensed to companies who wish to implement the tech in their product, called implementers, on Fair, Reasonable, and Non-Discriminatory (FRAND) terms. Current standards promote price gouging, FRAND enforcement is critical.

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)

I. Standard Setting and the Competitive Process

The fundamental economics in the information technology sector, driven by network effects, implies that there is enormous value associated with establishing compatibility standards. Popular standards include the mobile broadband standards used in cell phones, which are established by the 3rd Generation Partnership Project (3GPP), and the Wi-Fi technology for wireless local area networks, which is enabled by the 802.11 standard established by the Institute of Electrical and Electronics Engineers (IEEE).4

There are many SSOs, and their rules and procedures differ considerably. In addition to IEEE, leading SSOs include the International Organization for Standardization (ISO), the International Telecommunication Union (ITU), the European Telecommunications Standards Institute (ETSI), the Internet Engineering Task Force (IETF), and the World Wide Web Consortium (W3C).5 SSOs generally establish standards by holding a series of committee meetings among industry participants. These meetings culminate in a vote on a technical specification that describes what features or attributes a product must have in order to comply with the standard. Most SSOs are open to all industry participants and seek to operate on a consensus basis, applying certain voting rules. SSOs do not normally engage in patent licensing, nor do they specify how patent royalties will be divided up among patent holders. They leave that to their members, which in some cases form patent pools to address these issues.6

SSOs adopt specific policies relating to intellectual property rights (IPRs).7 These IPR policies are generally intended to enable the SEP holders to obtain reasonable royalties for licensing their patents, while prohibiting them from charging excessive royalties after other industry participants have committed to the standard. At that point, firms committed to implementing the standard— which we call “implementers”—would find it very costly to avoid using the patented technology. For this purpose, most SSOs require SEP owners to license their SEPs on FRAND terms.8

FRAND policies are especially necessary because negotiations between SEP holders and implementers generally take place only after the implementers have used and infringed the technologies claimed by the SEPs. Standards involving information and communications technology can involve hundreds or even thousands of SEPs, many with uncertain boundaries for infringement. In addition, a time lag exists between patent application and patent issuance. For these and other reasons, it is impractical for implementers to enter into negotiations for patent licenses with all SEP owners prior to the establishment of a standard and to their implementation of it.9

The fact that patent negotiations generally do not take place until after implementers have used and infringed the technologies has several critical implications. First, at the time of negotiation, implementers are locked into the standard and the technologies claimed by the SEPs—that is, the cost to switch to an alternative technology or standard at that point—ex post—is much greater than it was ex ante, before the patented technology was first included in the standard. Ex post, the patent holder is no longer competing to have its technology included in the standard, nor is it competing to have implementers of the standard use its technology. Instead, because the patent holder owns an asset that is essential to the standard, implementers have no choice but to use the patented technology.

If the standard is commercially successful, implementers are willing to pay a much larger royalty for use of the patented technology than they would have paid ex ante, when the SEP holder faced competition from other technologies. In these circumstances, the SEP holder can be said to have obtained monopoly power in the market in which the patented technology is licensed for use in implementing the standard.10

Second, because of lock-in and the implementer’s ongoing infringement, the potential for litigation looms large in licensing negotiations. In effect, the parties are negotiating about how to settle an infringement suit, and that negotiation is heavily influenced by their predictions as to what the court will do if they cannot agree. This situation is not unique to SEPs; it arises frequently when firms are faced with patent infringement claims for products they have independently developed or technologies they have inadvertently infringed. Patent law addresses such instances by specifying that patent holders are entitled to “reasonable royalties,” defined as the royalties that the parties would have negotiated prior to the infringement and thus prior to lock-in.11 Those hypothetical ex ante royalties reflect the market value of the patent license. Notwithstanding the law’s embrace of this principle, however, as a practical matter, patent holders are generally able to recover more than the ex ante value of the patent when litigation occurs after the implementers are locked in. Further, negotiations in the shadow of litigation after lock-in tend to result in royalties in excess of the ex ante or market value of the patented technology.12

Third, the shadow of litigation is particularly problematic in the communications and technology sector, in which products typically include hundreds or thousands of patented technologies. A court-ordered injunction involving such products would deprive the implementer of not only the value of the technology covered by the patent-in-suit, but also the value of the entire product.13 Implementers that are forced to bear the risk of an injunction are thus induced to agree to royalties greater than those that would be appropriate if only the value of the patented technology were at stake. Those royalties systematically provide SEP holders with excessive compensation in comparison with the benchmark of ex ante royalties.

These implications of lock-in and ex post dealings are well-understood: they represent an example of the general concept of lock-in and opportunism developed by Oliver Williamson.14 The Federal Circuit has also recognized the market distortions caused by the inclusion of patented technologies in public standards and the resulting danger of patent holdup involving SEPs.15

For these and other reasons, the SEP holder has ex post monopoly power that, if left unchecked, would enable it to obtain royalties far in excess of the royalties that it could earn in a competitive market.16 To address this common problem and limit ex post opportunism by SEP holders, SSOs typically require participants that own SEPs to make certain FRAND commitments. In particular, by requiring a commitment to license on “fair and reasonable” terms, the FRAND requirement aims to prevent, or at least reduce, the extent of monopoly pricing by SEP holders. And by requiring a commitment to license on “nondiscriminatory” terms, the FRAND requirement can prevent SEP holders from extracting monopoly premiums by selective licensing or, more important, migrating their monopoly power from the FRAND-regulated market to unregulated standard-implementing product markets by licensing to only one or a few implementers or licensing to selected implementers on discriminatorily favorable terms.

#### Patent holdup is accentuated by the Ninth Circuit’s recent decision in *FTC v. Qualcomm* that permits ICT firms to engage in innovation-stifling conduct with antitrust impunity.

Moss 20, \*Alex Moss is a Staff Attorney on EFF’s intellectual property team, before joining EFF, Alex practiced complex commercial litigation at Sullivan & Cromwell LLP in New York and Durie Tangri LLP in San Francisco; (August 26th, 2020, “Throwing Out the FTC's Suit Against Qualcomm Moves Antitrust Law in the Wrong Direction”, https://www.eff.org/deeplinks/2020/08/throwing-out-ftcs-suit-against-qualcomm-moves-antitrust-law-wrong-direction)

Standards can enhance competition and consumer choice, but they also massively inflate the value of patents deemed essential to the standard, and give their owners the power to sue companies that implement the standard for money damages or injunctions to block them from using their SEPs. When standards cover critical features like wireless connectivity, SEP owners wield a huge amount of “hold-up” power because their patents allow them to effectively block access to the standard altogether. That lets them charge unduly large tolls to anyone who wants to implement the standard.

To minimize that risk, standard-setting organizations typically require companies that want their patented technology incorporated into a standard to promise in advance to license their SEPs to others on fair, reasonable, and non-discriminatory (FRAND) terms. But that promise strikes at a key tension between antitrust and patent law: patent owners have no obligation to let anyone use technology their patent covers, but to get those technologies incorporated into standards, patent owners usually have to promise that they will give permission to anyone who wants to implement the standard as long as they pay a reasonable license fee.

Qualcomm is one of the most important and dominant companies in the history of wireless communication standards. It is a multinational conglomerate that has owned patents on every major wireless communication standard since its first CDMA patent in 1985, and it participates in the standard-setting organizations that define those standards. Qualcomm is somewhat unique in that it not only licenses SEPs, but also supplies the modem chips used by a wide range of devices. These include chips that implement wireless communication standards, which lie at the heart of every mobile computing device.

Although Qualcomm promised to license its SEPs (including patents essential to CDMA, 3G, 4G, and 5G) on FRAND terms, its conduct has to many looked unfair, unreasonable, and highly discriminatory. In particular, Qualcomm has drawn scrutiny for bundling tens of thousands of patents together—including many that are not standard-essential—and offering portfolio-only licenses no matter what licensees actually want or need; refusing to sell modem chips to anyone without a SEP license and threatening to withhold chips from companies trying to negotiate different license terms; refusing to license anyone other than original-equipment manufacturers (OEMs); and insisting on royalties calculated as a percentage of the sale price of a handset sold to end users for hundreds of dollars, despite the minimal contribution of any particular patent to the retail value.

In 2017, the U.S. Federal Trade Commission [sued](https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-qualcomm-monopolizing-key-semiconductor-device-used) Qualcomm for violating both sections of the Sherman Antitrust Act by engaging in a number of anticompetitive SEP licensing practices. In May 2019, the U.S. District Court for the Northern District of California agreed with the FTC, identifying numerous instances of Qualcomm’s unlawful, anticompetitive conduct in a comprehensive [233-page opinion](https://www.eff.org/document/ftc-v-qualcomm-district-court-opinion). We were pleased to see the FTC take action and the district court credit the overwhelming evidence that Qualcomm’s conduct is corrosive to market-based competition and threatens to cement Qualcomm’s dominance for years to come.

But this month, a panel of judges from the Court of Appeals for the Ninth Circuit unanimously [overturned](https://www.eff.org/document/ninth-circuit-opinion-ftc-v-qualcomm) the district court’s decision, reasoning that Qualcomm’s conduct was “hypercompetitive” but not “anticompetitive,” and therefore not a violation of antitrust law. To reach that result, the Ninth Circuit made the patent grant more powerful and antitrust law weaker than ever.

According to the Ninth Circuit, patent owners don’t have a duty to let anyone use what their patent covers, and therefore Qualcomm had no duty to license its SEPs to anyone. But that framing requires ignoring the promises Qualcomm made to license its SEPs on reasonable and non-discriminatory terms—promises that courts in this country and around the world have consistently enforced. It also means ignoring antitrust principles like the essential facilities doctrine, which limits the ability of a monopolist with hold-up power over an essential facility (like a port) to shut out rivals. Instead, the Ninth Circuit held rather simplistically that a duty to deal could arise only if the monopolist had provided access, and then reversed its policy.

But even when Qualcomm restricted its licensing policies in critical ways, the Ninth Circuit found reasons to approve those restrictions. For example, Qualcomm stopped licensing its patents to chip manufacturers and started licensing them only to OEMs. This had a major benefit: it let Qualcomm charge a much higher royalty rate based on the high retail price of the end user devices, like smartphones and tablets, that OEMs make and sell. If Qualcomm had continued to license to chip suppliers, its patents would be “exhausted” once the chips were sold to OEMs, extinguishing Qualcomm’s right to assert its patents and control how the chips were used.

Patent exhaustion is a century-old doctrine that protects the rights of consumers to use things they buy without getting the patent owner’s permission again and again. Patent exhaustion is important because it prevents price-gouging, but also because it protects space for innovation by letting people use things they buy freely, including to build innovations of their own. The doctrine thus helps patent law serve its underlying goal—promoting economic growth and innovation. In other words, the doctrine of exhaustion is baked into the patent grant; it is not optional. Nevertheless, the Ninth Circuit wholeheartedly approved of Qualcomm’s efforts to avoid exhaustion—even when that meant cutting off access to previous licensees (chip-makers) in ways that let Qualcomm charge far more in licensing fees than its SEPs could possibly have contributed to the retail value of the final product.

It makes no sense that Qualcomm could contract around a fundamental principle like patent exhaustion, but at the same time did not assume any antitrust duty to deal under these circumstances. Worse, it’s harmful for the economy, innovation, and consumers. Unfortunately, the kind of harm that antitrust law recognizes is limited to harm affecting “competition” or the “competitive process.” Antitrust law, at least as the Ninth Circuit interprets it, doesn’t do nearly enough to address the harm downstream consumers experience when they pay inflated prices for high-tech devices, and miss out on innovation that might have developed from fair, reasonable, and non-discriminatory licensing practices.

We hope the FTC sticks to its guns and asks the Ninth Circuit to go en banc and reconsider this decision. Otherwise, antitrust law will become an even weaker weapon against innovation-stifling conduct in technology markets.

#### Weakened antitrust enforcement emboldens firms to follow Qualcomm’s lead, which collapses FRAND integrity.

Hovenkamp 20, \*Herbert J. Hovenkamp is James G. Dinan University Professor at the University of Pennsylvania Law School and the Wharton School of the University of Pennsylvania; (2020, “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.

While governments can be heavily involved in standard set-ting,9 the implementation of technical standards in information technologies is largely the work of private actors. Government involvement is limited mainly to enforcement of contract, intellectual property, or antitrust law. As private actors, those involved in standard setting or compliance are fully subject to the federal antitrust laws.

This Article addresses one question: when is an SSO participant’s violation of a FRAND commitment an antitrust violation, and if it is, of what kind and what are the implications for remedies? It warns against two extremes. One is thinking that any violation of a FRAND commitment is an antitrust violation as well. In the first instance FRAND obligations are contractual, and most breaches of contract do not violate any antitrust law. The other extreme is thinking that, because a FRAND violation is a breach of contract, it cannot also be an antitrust violation. The question of an antitrust violation does not de-pend on whether the conduct breached a particular agreement but rather on whether it caused competitive harm. This can happen because the conduct restrained trade under section 1 of the Sherman Act, was unreasonably exclusionary under section 2 of the Sherman Act, or amounted to an anticompetitive condition or understanding as defined by section 3 of the Clay-ton Act.10 The end goal is to identify practices that harm com-petition, thereby injuring consumers.

The Ninth Circuit’s Qualcomm decision will make antitrust violations in the context of FRAND licensing much more difficult to prove, even in cases where anticompetitive behavior and consumer harm seem clear.11 Indeed, in this case the court itself acknowledged the harm to consumers but appeared to think that they were not entitled to protection.12 If this decision stands, FRAND obligations will to a larger extent have to be settled through private litigation and the federal antitrust enforcement agencies will have a diminished role. Anticompetitive behavior by one firm that is not effectively disciplined will lead others to do the same thing.

#### Monopoly pricing and selective licensing undermines 5G innovation---FRAND enforcement is key.

Actonline 20, the App Association represents more than 5,000 app companies and information technology firms across the mobile economy; (August 26th, 2020, “Save Our Standards: The Ninth Circuit Court of Appeals Reverses Decision in FTC v. Qualcomm”, <https://actonline.org/2020/08/26/save-our-standards-the-ninth-circuit-court-of-appeals-reverses-decision-in-ftc-v-qualcomm/>)

* Ability edited

Moreover, the FRAND agreement is a critical tool used by standard setting organizations to ensure the process enhances competition and does not run afoul of antitrust laws. Generally, a collaboration between competitors to choose market winners or set prices raises significant questions for competition regulators. Royalty free and FRAND licensing requirements were created by standards bodies to avoid potential antitrust scrutiny by limiting the market power and the potential for abuse by those involved in developing a standard. This is why the American National Standards Institute (ANSI) will not accredit any standards developing organization (SDO) that does not require standard-essential patent holders to provide licensing terms at least as favorable as FRAND.

The most important beneficiary of open interoperability standards and FRAND licensing requirements are the entrepreneurs and small businesses that have long fueled America’s innovation engine. They don’t have giant patent portfolios, market power, or the resources to hire legions of lawyers and spend years battling SEP abusers in civil court. Without some level of certainty about their ability to obtain licenses—let alone what they may cost—entrepreneurs will have trouble justifying the pursuit of any innovation that uses a standard and will certainly struggle to raise money from investors for such innovation. And Qualcomm’s vague and toothless promise simply “not to sue” smaller companies and component makers is no substitute for a license.

The adoption of 5G technology is expected to open unprecedented opportunities for innovation and economic growth as we move toward a world where everything from cars to tractors to buildings will connect to wireless networks. At every stage of the information technology revolution, America has been the undisputed leader because of the unparalleled entrepreneurial innovation ecosystem that we have built. If 5G SEP holders are able to arbitrarily refuse licenses to smaller firms, it would ~~cripple~~ undermine America’s innovation ecosystem at the start of the next big wave of innovation. As economic tensions continue to rise with China, Chinese-based companies could use their 5G SEPs as international economic weapons to thwart U.S. competitors.

The 5G standard is supposed to be a platform for competition, innovation, and entrepreneurship, but if the Ninth Circuit decision is allowed to stand, it will become a chokepoint for snuffing out competitors and demanding monopoly rents. Open standards and FRAND licensing commitments are fundamental to competition in the modern economy, and the idea that they aren’t a subject for antitrust enforcement is patently absurd.

#### The absence of domestic 5G competition cedes leadership in technical standards to China.

Duan 19, \*Charles Duan is a senior fellow and associate director of tech & innovation policy at the R Street Institute, where he focuses his research on intellectual property issues; (February 5th, 2019, “Why China Is Winning the 5G War”, https://nationalinterest.org/feature/why-china-winning-5g-war-43347)

There is little doubt today that American superiority in the next generation of mobile communications, commonly called 5G, is a matter of extraordinary national concern. There is also little doubt that China is a strong competitor, already having outspent the United States by [$24 billion](https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-5g-deployment-imperative.pdf#page=3) and planning [$411 billion](https://www.scmp.com/tech/china-tech/article/2098948/china-plans-28-trillion-yuan-capital-expenditure-create-worlds) in 5G investment over the next decade. The Chinese government has also laid out multiple national plans for establishing the country as a leader in mobile technology, and the Chinese firm Huawei is poised to be the [top smartphone manufacturer](https://www.cnbc.com/2018/11/16/huawei-aims-to-overtake-samsung-as-no-1-smartphone-player-by-2020.html) by 2020.

And what are United States companies doing about this? Bickering over patents.

For years, the leading American supplier of advanced mobile communications chips has been the San Diego-based Qualcomm. The company has been an innovator of mobile technology, but it has also been a remarkable innovator of convoluted legal strategies. As an ongoing Federal Trade Commission [lawsuit alleges](https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-qualcomm-monopolizing-key-semiconductor-device-used), Qualcomm has used its dominant position as a chip supplier and its extensive patent holdings to weave an intricate web of patent licensing across the mobile industry. The effect of that complex licensing scheme, the FTC claims, has been to force competitor chipmakers out of the market and to extract concessions and high patent royalties from smartphone and mobile-device makers.

Qualcomm today faces only one major U.S. competitor—Intel, whose chips Apple recently [started using](https://www.cultofmac.com/484250/intel-reaping-rewards-apples-scrap-qualcomm/) instead of Qualcomm’s. Not surprisingly, Qualcomm has leveraged its patents to force a retaliatory investigation against Apple, the effect of which could be, as an administrative judge [recently determined](http://www.fosspatents.com/2018/10/itc-judge-didnt-buy-testimony-for-which.html), to boot Intel out of the mobile-chip market and leave Qualcomm as a monopoly.

It is hard to imagine that this infighting among Apple, Intel and Qualcomm is getting the United States very far in 5G, and it is harder to imagine that Qualcomm’s desired outcome would do so, either. The best path, instead, is the obvious one: allowing competition and expanding the number of firms working on 5G.

Competition encourages companies to out-innovate each other in order to grab market share. Of particular importance to 5G, competition leads to [better cybersecurity](https://morningconsult.com/opinions/in-the-race-to-5g-monopoly-considered-harmful/) in products, making them less vulnerable to hacking or misuse.

Competition is especially crucial when it comes to the technical standards that define how 5G works. These standards are the work of 3GPP, an international consortium of technology companies in the field. Chinese players such as Huawei and ZTE are major participants in 3GPP. Ensuring that 3GPP’s standards reflect American values requires having as many American companies at the negotiating table as possible—which is harder to achieve when those companies are trying to sue each other out of business.

Certainly patents themselves, as rewards for new inventions, are a driver of innovation in areas such as 5G. The problem, though, is not the existence of a patent system but the ever-expanding power of the patent laws, which encourage companies to pour dollars into complex patent licensing and assertion schemes—as companies like Qualcomm have done—rather than to perform the hard work of building new technologies. When innovation in patent strategy is more profitable than actual innovation, we lose the race to 5G and other technologies.

But don’t take my word for it. [Multiple members of Congress](https://www.patentprogress.org/2019/01/11/congress-weighs-in-on-qualcomm-and-apple-at-the-itc/), from both sides of the aisle, have denounced the use of patents to kick companies like Intel out of 5G development, predicting that such actions would “dampen the quality, innovation, competitive pricing, and in this case the preservation of a strong U.S. presence in the development of 5G and thus the national security of the United States.”

Or look to what China itself is doing. The Chinese government is handing out rewards left and right to encourage technology research and development. Indeed, it grants subsidies and financial benefits (ranging from the [ordinary](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2818503) to the [imperfect](https://funginstitute.berkeley.edu/wp-content/uploads/2013/12/patent_subsidy_Zhen.pdf) to the [bizarre](https://www.scmp.com/news/china/article/1681850/how-get-out-jail-early-china-buy-inventors-idea-and-patent-it)) to encourage its citizens to file for patents. But while China specifically encourages filing for patents, it does little to encourage using them: Patent infringement awards in court are peanuts—often only [five figures](https://scholarship.law.berkeley.edu/btlj/vol33/iss2/2/)—and most Chinese patent owners drop their patents [within five years](https://www.bloomberg.com/news/articles/2018-09-26/china-claims-more-patents-than-any-country-most-are-worthless) of getting them. The message in China is clear: You will be rewarded for innovating, but not for quibbling over patents.

The United States should take the same tack if it wants to match China in 5G. Ever-stronger patent rights encourage counterproductive disputes that are a drag on industry, a drag on research and development, and ultimately a drag on domestic competitiveness on the global stage. If America wants to lead in 5G, then it must clear the path for strong competition among leading American technology companies.

#### Standards leadership allows China to export digital authoritarianism.

Drew et al. 21, \*Dr Alexi Drew, Research Associate, The Policy Institute, King’s College London; (May 7th, 2021, “The Critical Geopolitics of Standards Setting”, https://www.transatlantic-dialogue-on-china.rusi.org/article/the-critical-geopolitics-of-standards-setting)

However, this previously ‘western’ domain is challenged by a Chinese bloc of private industry actors with centrally directed, strategic motivations for their efforts who have managed to leverage the flaws of this system for political and economic advantage.  The market-driven self-regulation model of technical standards has proven itself unsustainable given the geopolitical power achievable through the control of these standards. The marketised approach is easily abusable by a technologically developed nation-state with geopolitical intentions firmly in mind.

Obscurity Through Complexity

Technical standards have the immediate appearance of being both apolitical and ethically neutral. This seems to set them apart from the debate over standards of state behaviour in [cyber space concerning espionage and actions below the threshold of armed conflict](https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what). Yet, technological standards are unequivocally connected to normative practices of international behaviour and ethics. The extremely complex nature of the standards under consideration in bodies such as the International Organization for Standardization, the International Electrotechnical Commission (IEC), the International Telecommunications Union (ITU), and the Third Generation Partnership Project (3GPP) obscures the very tangible real-world impact that the standards they set have. The 3GPP is responsible for standards setting for mobile telecommunications. It covers everything from 5G through to autonomous vehicles and the Internet of Things. These are the bodies defining how the modern world is constructed.

On the one hand they appear quite benign, responsible for such banalities as the use of Universal Serial Bus (USB) connectors versus proprietary standards. This hardly seems a matter of national security importance. But the same process is responsible for what ultimately shape the basic operating parameters of facial recognition technology in closed circuit television systems, the level of centralised state control at the technical foundations of the internet, and the protections of personally identifiable data. These generate profound implications for international policy and ethics.

Internal Competition vs Strategic Direction

Technical standards setting processes have, historically, been dominated by private sector actors who have had both the capacity to develop a particular technology to the point of holding a significant market share, and the ability to use that market share to advocate for the standardisation of the technology in line with their own production. The market led approach has continued to be the prevailing model by which American companies have globalised the technical standards behind US dominated technological innovation. This privatised form of self-regulation for technology companies is only partially influenced by the approach taken within the EU where [some licensing of standards are controlled by state or EU led institutions.](https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2019/ui-brief-no.-2-2019.pdf)

In contrast to this approach the Chinese model has involved a high level of state-oriented direction, oversight, and direct engagement on the creation and signing off technical standards. Efforts to harmonise and centralise technical standards domestically have become increasingly internationalised as the CCP takes this centralised, strategic approach to technical standards setting bodies such as the ITU, 3GPP, and IEC. Technical standards have also become an increasingly central component of the Digital Silk Road with the openly expressed goal of increasing uptake of Chinese technical standards in partner countries.

The implications of this clash between a system of technical standardisation that is driven by the market versus one driven by an authoritarian government subsidised model are a direct challenge to the development of free, open, and ethical technology. Standardisation mechanisms have become political, or rather there has been a gradual realisation of the political power to be gained from the control of technical standards. While the PRC might have come to this awareness first, the US and Europe have since had a rude awakening about the missed opportunity. The privatised model of technical standards setting favoured by European and US markets relies upon the dynamics of financial competition to regulate behaviour. This is in stark contrast to the statist Chinese model.

#### Causes global backsliding.

Kendall-Taylor et. al 20 \*Andrea Kendall-Taylor, senior fellow and director of the Transatlantic Security Program at the Center for a New American Security, co-author of Democracies and Authoritarian Regimes; Erica Frantz is Assistant Professor of Political Science at Michigan State University; Joseph Wright is Professor of Political Science at Pennsylvania State University; (March/April 2020, “The Digital Dictators,” Foreign Affairs, <https://www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators>)

The risk that technology will usher in a wave of authoritarianism is all the more concerning because our own empirical research has indicated that beyond buttressing autocracies, digital tools are associated with an increased risk of democratic backsliding in fragile democracies. New technologies are particularly dangerous for weak democracies because many of these digital tools are dual use: technology can enhance government efficiency and provide the capacity to address challenges such as crime and terrorism, but no matter the intentions with which governments initially acquire such technology, they can also use these tools to muzzle and restrict the activities of their opponents.

#### Democracy solves a litany of existential threats.

Diamond 19, Professor of Political Science and Sociology at Stanford University, Senior Fellow at the Hoover Institution, Senior Fellow at the Freeman Spogli Institute for International Studies, PhD in Sociology from Stanford University, (Dr. Larry, Ill Winds: Saving Democracy from Russian Rage, Chinese Ambition, and American Complacency, p. 199-202)

The most obvious response to the ill winds blowing from the world’s autocracies is to help the winds of freedom blowing in the other direction. The democracies of the West cannot save themselves if they do not stand with democrats around the world. This is truer now than ever, for several reasons. We live in a globalized world, one in which models, trends, and ideas cascade across borders. Any wind of change may gather quickly and blow with gale force. People everywhere form ideas about how to govern—or simply about which forms of government and sources of power may be irresistible—based on what they see happening elsewhere. We are now immersed in a fierce global contest of ideas, information, and norms. In the digital age, that contest is moving at lightning speed, shaping how people think about their political systems and the way the world runs. As doubts about and threats to democracy are mounting in the West, this is not a contest that the democracies can afford to lose. Globalization, with its flows of trade and information, raises the stakes for us in another way. Authoritarian and badly governed regimes increasingly pose a direct threat to popular sovereignty and the rule of law in our own democracies. Covert flows of money and influence are subverting and corrupting our democratic processes and institutions. They will not stop just because Americans and others pretend that we have no stake in the future of freedom in the world. If we want to defend the core principles of self-government, transparency, and accountability in our own democracies, we have no choice but to promote them globally. It is not enough to say that dictatorship is bad and that democracy, however flawed, is still better. Popular enthusiasm for a lesser evil cannot be sustained indefinitely. People need the inspiration of a positive vision. Democracy must demonstrate that it is a just and fair political system that advances humane values and the common good. To make our republics more perfect, established democracies must not only adopt reforms to more fully include and empower their own citizens. They must also support people, groups, and institutions struggling to achieve democratic values elsewhere. The best way to counter Russian rage and Chinese ambition is to show that Moscow and Beijing are on the wrong side of history; that people everywhere yearn to be free; and that they can make freedom work to achieve a more just, sustainable, and prosperous society. In our networked age, both idealism and the harder imperatives of global power and security argue for more democracy, not less. For one thing, if we do not worry about the quality of governance in lower-income countries, we will face more and more troubled and failing states. Famine and genocide are the curse of authoritarian states, not democratic ones. Outright state collapse is the ultimate, bitter fruit of tyranny. When countries like Syria, Libya, and Afghanistan descend into civil war; when poor states in Africa cannot generate jobs and improve their citizens’ lives due to rule by corrupt and callous strongmen; when Central American societies are held hostage by brutal gangs and kleptocratic rulers, people flee—and wash up on the shores of the democracies. Europe and the United States cannot withstand the rising pressures of immigration unless they work to support better, more stable and accountable government in troubled countries. The world has simply grown too small, too flat, and too fast to wall off rotten states and pretend they are on some other planet. Hard security interests are at stake. As even the Trump administration’s 2017 National Security Strategy makes clear, the main threats to U.S. national security all stem from authoritarianism, whether in the form of tyrannies from Russia and China to Iran and North Korea or in the guise of antidemocratic terrorist movements such as ISIS.1 By supporting the development of democracy around the world, we can deny these authoritarian adversaries the geopolitical running room they seek. Just as Russia, China, and Iran are trying to undermine democracies to bend other countries to their will, so too can we contain these autocrats’ ambitions by helping other countries build effective, resilient democracies that can withstand the dictators’ malevolence. Of course, democratically elected governments with open societies will not support the American line on every issue. But no free society wants to mortgage its future to another country. The American national interest would best be secured by a pluralistic world of free countries—one in which autocrats can no longer use corruption and coercion to gobble up resources, alliances, and territory. If you look back over our history to see who has posed a threat to the United States and our allies, it has always been authoritarian regimes and empires. As political scientists have long noted, no two democracies have ever gone to war with each other—ever. It is not the democracies of the world that are supporting international terrorism, proliferating weapons of mass destruction, or threatening the territory of their neighbors.

#### China 5G leadership compromise US military superiority

Borghard et al. 19, \*Erica D. Borghard is an Assistant Professor at the Army Cyber Institute at West Point. Shawn W. \*Lonergan is a U.S. Army Reserve officer assigned to 75th Innovation Command and a Research Scholar at the Army Cyber Institute. (April 25th, 2019, “The Overlooked Military Implications of the 5G Debate”, https://www.cfr.org/blog/overlooked-military-implications-5g-debate)

There are economic implications for which entities can secure the [greatest global market share](https://www.reuters.com/brandfeatures/venture-capital/article?id=61837) of 5G technology. Technological innovation drives economic growth, job creation, and global economic influence. Huawei may have a long-term market advantage over U.S and Western telecoms because the former has been able to offer 5G products at [far cheaper](https://www.nytimes.com/2019/01/26/us/politics/huawei-china-us-5g-technology.html) rates than the latter. Furthermore, there are also concerns that Chinese-built 5G technology is likely to [contain backdoors](https://www.wired.com/story/huawei-case-signals-new-us-china-cold-war-tech/) that could be used to enable [Chinese economic or national security espionage](https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html). It is unlikely that Beijing would actively monitor all of the content of the data that comes across Huawei owned or operated infrastructure (although it may collect and analyze metadata). However, it is conceivable that Huawei would get a proverbial “tap on the shoulder” from Beijing to share pertinent information in specific instances. This may include individually targeting senior corporate executives, which is enabled by the millimeter wave frequency that 5G networks employ.

The military applications of 5G technology have vital strategic and battlefield implications for the U.S. Historically, the U.S. military has reaped enormous advantages from employing cutting edge technology on the battlefield. 5G technology holds similar innovative potential. Perhaps most obviously, the next generation of telecommunications infrastructure will have a direct impact on improving military communications. However, it will also produce cascading effects on the development of other kinds of military technologies, such as robotics and artificial intelligence. For instance, artificial intelligence and machine learning capabilities, such as those used in the Department of Defense’s [Project Maven](https://dod.defense.gov/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/), could be greatly enhanced when leveraging the data processing speeds made possible through 5G infrastructure. As an [era of great power competition](https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf) emerges between the United States and China, the United States has a compelling strategic interest in being at the forefront of these new technologies.

The United States and its allies must also consider the tactical and operational implications on the battlefield of conducting conventional or counterinsurgency operations in an area with Chinese owned or operated 5G infrastructure. This concern stems from the nature of the relationship between Huawei, an [ostensibly private company](https://www.itnews.com.au/news/analysis-who-really-owns-huawei-175946), and the Chinese Communist Party (CCP). While Huawei’s founder and CEO, Ren Zhengfei proclaimed in a February 2019 interview on [CBS This Morning](https://www.cbsnews.com/news/ren-zhengfei-huawei-ceo-says-we-will-never-provide-chinese-government-with-any-information/)that the company never has and never would provide information to the Chinese government, many experts are [skeptical](https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html). Under China’s [2017 National Intelligence Law](https://www.reuters.com/article/us-china-security-lawmaking-idUSKBN19I1FW), the CCP has the authority to monitor and investigate domestic and international companies as well as direct organizations to assist with government espionage efforts. As such, it is conceivable that Huawei will be required to hand over its data to the Chinese government for collection and analysis.

Due to this reality, the United States must consider and be prepared to conduct overseas contingency or counterterrorism operations in areas where Chinese telecommunications infrastructure is widely proliferated, thus restricting the United States’ ability to rely on indigenous telecoms. As [noted](https://www.africom.mil/media-room/transcript/31604/gen-joseph-votel-gen-thomas-waldhauser-and-acting-asd-for-international-security-affairs-kathryn) by US AFRICOM Commander General Thomas Waldhauser, this has already become an issue in Africa where Chinese telecommunications companies are poised to dominate. The integrity of U.S. military communications systems that rely on 5G networks could be undermined at key phases of an operation. For example, if the United States is conducting a military operation in an area of interest to China, it is plausible that the Chinese government could leverage Huawei to intercept or even deny military communications. Furthermore, Chinese telecom infrastructure dominance in a theater of operations may limit the U.S. military’s ability to conduct precision targeting that leverages signals intelligence collection on 5G telecommunications networks.

The strategic and battlefield implications of who owns and operates 5G infrastructure around the world underscores the national security importance of 5G. The U.S. government and its allies should more systematically assess both the opportunities and risks associated with conducting future military operations in environments that rely on Chinese technology.

To date, the U.S. government has devoted significant energy to persuading its allies and partners to follow the United States in prohibiting Chinese telecoms, particularly Huawei, from building and/or operating 5G infrastructure. However, its diplomatic approach has been met with varying degrees of success. While some countries such as [Australia](https://www.ft.com/content/e90c3800-aad3-11e8-94bd-cba20d67390c) and [Japan](https://www.reuters.com/article/us-usa-china-huawei-japan/japans-top-three-telcos-to-exclude-huawei-zte-network-equipment-kyodo-idUSKBN1O90JW) have fallen in line with the U.S. stance on Huawei, many others have not. The European Commission’s recent 5G [recommendations](https://www.cyberscoop.com/5g-eu-huawei-cybersecurity-recommendations/) for member states dismissed a ban on Chinese telecoms. British intelligence has reportedly maintained that the security risks associated with Huawei can be [sufficiently managed](https://www.ft.com/content/619f9df4-32c2-11e9-bd3a-8b2a211d90d5), and New Zealand, after [initially bandwagoning](https://www.nytimes.com/2018/11/28/business/huawei-new-zealand-papua-new-guinea.html) with the United States in December 2018, abruptly [reversed course](https://www.bloomberg.com/news/articles/2019-02-18/new-zealand-says-china-s-huawei-hasn-t-been-ruled-out-of-5g-role) in February 2019. This is concerning for the United States because New Zealand and the UK are members of the Five Eyes intelligence-sharing alliance. Many allies have refused an outright ban of Huawei because of the company’s ability to offer 5G products at far cheaper rates than Western telecoms.

It is clear that U.S. diplomatic efforts are not working. The reality is that the bottom line is largely driving decision-making. Therefore, rather than take a purely negative approach, the United States should consider using positive inducements to make its 5G products more appealing. While the United States should not strive to mirror China’s top-down approach to innovation, it should work with allies to use market incentives to make U.S.- and Western-developed 5G infrastructure and products more competitive. Furthermore, the U.S. military needs to anticipate that its use of native telecommunications infrastructure in a future operating environment may be compromised, limited, or denied. The U.S. military will inevitably need greater bandwidth on the tactical edge and this should be an imperative that drives investment in research and development to address this challenge.

Technological innovation was at the crux of the United States’ comparative military and economic advantage in the twentieth century. In this contemporary great power competition, U.S. failure to innovate at the scientific and technological frontier will have direct (and deleterious) effects for the United States on the distribution of power in the international system over the long term.

#### Chinese tech superiority upends deterrence and emboldens them to risk conflict over Taiwan---extinction.

Kroenig 18, Deputy Director for Strategy, Scowcroft Center for Strategy and Security Associate Professor of Government and Foreign Service, Georgetown University (Matthew, Nov 12, 2018, “Will disruptive technology cause nuclear war?” *BAS*, <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.

When it comes to new technology, this means that the United States should seek to maintain an innovation edge. Washington should also work with other states, including its nuclear-armed rivals, to develop a new set of arms control and nonproliferation agreements and export controls to deny these newer and potentially destabilizing technologies to potentially hostile states.

These are no easy tasks, but the consequences of Washington losing the race for technological superiority to its autocratic challengers just might mean nuclear Armageddon.

### 1AC---Cybersecurity ADV

#### Advantage 2 is Cybersecurity:

#### Aggressive patent strategies create structural flaws in 5G standardization that imperils domestic cybersecurity---market competition reduces the incidence of vulnerability and severity of attacks.

Duan 20, \*Charles Duan is a senior fellow and associate director of tech & innovation policy at the R Street Institute, where he focuses his research on intellectual property issues; (2020, “OF MONOPOLIES AND MONOCULTURES: THE INTERSECTION OF PATENTS AND NATIONAL SECURITY”, Santa Clara High Technology Law Journal, 36(4), 369-405. Retrieved from <https://www2.lib.ku.edu/login?url=https://www.proquest.com/scholarly-journals/monopolies-monocultures-intersection-patents/docview/2442966690/se-2?accountid=14556>)

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.156 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.157 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.159 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.160 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.”163 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.”167

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.170 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.

#### 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/" \l "_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/" \l "_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/" \l "_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/" \l "_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/" \l "_ftn14)

#### Those attacks cause accidental nuclear escalation.

Klare 19, \*Michael T. Klare is a professor emeritus of peace and world security studies at Hampshire College and senior visiting fellow at the Arms Control Association; (November 19th, “Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation”, https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation)

Yet another pathway to escalation could arise from a cascading series of cyberstrikes and counterstrikes against vital national infrastructure rather than on military targets. All major powers, along with Iran and North Korea, have developed and deployed cyberweapons designed to disrupt and destroy major elements of an adversary’s key economic systems, such as power grids, financial systems, and transportation networks. As noted, Russia has infiltrated the U.S. electrical grid, and it is widely believed that the United States has done the same in Russia.[12](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote12) The Pentagon has also devised a plan known as “Nitro Zeus,” intended to immobilize the entire Iranian economy and so force it to capitulate to U.S. demands or, if that approach failed, to pave the way for a crippling air and missile attack.[13](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote12)

The danger here is that economic attacks of this sort, if undertaken during a period of tension and crisis, could lead to an escalating series of tit-for-tat attacks against ever more vital elements of an adversary’s critical infrastructure, producing widespread chaos and harm and eventually leading one side to initiate kinetic attacks on critical military targets, risking the slippery slope to nuclear conflict. For example, a Russian cyberattack on the U.S. power grid could trigger U.S. attacks on Russian energy and financial systems, causing widespread disorder in both countries and generating an impulse for even more devastating attacks. At some point, such attacks “could lead to major conflict and possibly nuclear war.”[14](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote14)

These are by no means the only pathways to escalation resulting from the offensive use of cyberweapons. Others include efforts by third parties, such as proxy states or terrorist organizations, to provoke a global nuclear crisis by causing early-warning systems to generate false readings (“spoofing”) of missile launches. Yet, they do provide a clear indication of the severity of the threat. As states’ reliance on cyberspace grows and cyberweapons become more powerful, the dangers of unintended or accidental escalation can only grow more severe.

#### Cyber-compromised NC3 causes nuclear war.

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

The Nuclear-Cyber Connection

These links exist because the NC3 systems of the United States and other nuclear-armed states are heavily dependent on computers and other digital processors for virtually every aspect of their operation and because those systems are highly vulnerable to cyberattack. Every nuclear force is composed, most basically, of weapons, early-warning radars, launch facilities, and the top officials, usually presidents or prime ministers, empowered to initiate a nuclear exchange. Connecting them all, however, is an extended network of communications and data-processing systems, all reliant on cyberspace. Warning systems, ground- and space-based, must constantly watch for and analyze possible enemy missile launches. Data on actual threats must rapidly be communicated to decision-makers, who must then weigh possible responses and communicate chosen outcomes to launch facilities, which in turn must provide attack vectors to delivery systems. All of this involves operations in cyberspace, and it is in this domain that great power rivals seek vulnerabilities to exploit in a constant struggle for advantage.

The use of cyberspace to gain an advantage over adversaries takes many forms and is not always aimed at nuclear systems. China has been accused of engaging in widespread cyberespionage to steal technical secrets from U.S. firms for economic and military advantages. Russia has been accused, most extensively in the Robert Mueller report, of exploiting cyberspace to interfere in the 2016 U.S. presidential election. Nonstate actors, including terrorist groups such as al Qaeda and the Islamic State group, have used the internet for recruiting combatants and spreading fear. Criminal groups, including some thought to be allied with state actors, such as North Korea, have used cyberspace to extort money from banks, municipalities, and individuals.[4](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote04) Attacks such as these occupy most of the time and attention of civilian and military cybersecurity organizations that attempt to thwart such attacks. Yet for those who worry about strategic stability and the risks of nuclear escalation, it is the threat of cyberattacks on NC3 systems that provokes the greatest concern.

This concern stems from the fact that, despite the immense effort devoted to protecting NC3 systems from cyberattack, no enterprise that relies so extensively on computers and cyberspace can be made 100 percent invulnerable to attack. This is so because such systems employ many devices and operating systems of various origins and vintages, most incorporating numerous software updates and “patches” over time, offering multiple vectors for attack. Electronic components can also be modified by hostile actors during production, transit, or insertion; and the whole system itself is dependent to a considerable degree on the electrical grid, which itself is vulnerable to cyberattack and is far less protected. Experienced “cyberwarriors” of every major power have been working for years to probe for weaknesses in these systems and in many cases have devised cyberweapons, typically, malicious software (malware) and computer viruses, to exploit those weaknesses for military advantage.[5](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote05)

Although activity in cyberspace is much more difficult to detect and track than conventional military operations, enough information has become public to indicate that the major nuclear powers, notably China, Russia, and the United States, along with such secondary powers as Iran and North Korea, have established extensive cyberwarfare capabilities and engage in offensive cyberoperations on a regular basis, often aimed at critical military infrastructure. “Cyberspace is a contested environment where we are in constant contact with adversaries,” General Paul M. Nakasone, commander of the U.S. Cyber Command (Cybercom), told the Senate Armed Services Committee in February 2019. “We see near-peer competitors [China and Russia] conducting sustained campaigns below the level of armed conflict to erode American strength and gain strategic advantage.”

Although eager to speak of adversary threats to U.S. interests, Nakasone was noticeably but not surprisingly reluctant to say much about U.S. offensive operations in cyberspace. He acknowledged, however, that Cybercom took such action to disrupt possible Russian interference in the 2018 midterm elections. “We created a persistent presence in cyberspace to monitor adversary actions and crafted tools and tactics to frustrate their efforts,” he testified in February. According to press accounts, this included a cyberattack aimed at paralyzing the Internet Research Agency, a “troll farm” in St. Petersburg said to have been deeply involved in generating disruptive propaganda during the 2016 presidential elections.[6](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote06)

Other press investigations have disclosed two other offensive operations undertaken by the United States. One called “Olympic Games” was intended to disrupt Iran’s drive to increase its uranium-enrichment capacity by sabotaging the centrifuges used in the process by infecting them with the so-called Stuxnet virus. Another left of launch effort was intended to cause malfunctions in North Korean missile tests.[7](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote07) Although not aimed at either of the U.S. principal nuclear adversaries, those two attacks demonstrated a willingness and capacity to conduct cyberattacks on the nuclear infrastructure of other states.

Efforts by strategic rivals of the United States to infiltrate and eventually degrade U.S. nuclear infrastructure are far less documented but thought to be no less prevalent. Russia, for example, is believed to have planted malware in the U.S. electrical utility grid, possibly with the intent of cutting off the flow of electricity to critical NC3 facilities in the event of a major crisis.[8](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote08) Indeed, every major power, including the United States, is believed to have crafted cyberweapons aimed at critical NC3 components and to have implanted malware in enemy systems for potential use in some future confrontation.

Pathways to Escalation

Knowing that the NC3 systems of the major powers are constantly being probed for weaknesses and probably infested with malware designed to be activated in a crisis, what does this say about the risks of escalation from a nonkinetic battle, that is, one fought without traditional weaponry, to a kinetic one, at first using conventional weapons and then, potentially, nuclear ones? None of this can be predicted in advance, but those analysts who have studied the subject worry about the emergence of dangerous new pathways for escalation. Indeed, several such scenarios have been identified.[9](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote09)

The first and possibly most dangerous path to escalation would arise from the early use of cyberweapons in a great power crisis to ~~paralyze~~ undermine the vital command, control, and communications capabilities of an adversary, many of which serve nuclear and conventional forces. In the “fog of war” that would naturally ensue from such an encounter, the recipient of such an attack might fear more punishing follow-up kinetic attacks, possibly including the use of nuclear weapons, and, fearing the loss of its own arsenal, launch its weapons immediately. This might occur, for example, in a confrontation between NATO and Russian forces in east and central Europe or between U.S. and Chinese forces in the Asia-Pacific region.

Speaking of a possible confrontation in Europe, for example, James N. Miller Jr. and Richard Fontaine wrote that “both sides would have overwhelming incentives to go early with offensive cyber and counter-space capabilities to negate the other side’s military capabilities or advantages.” If these early attacks succeeded, “it could result in huge military and coercive advantage for the attacker.” This might induce the recipient of such attacks to back down, affording its rival a major victory at very low cost. Alternatively, however, the recipient might view the attacks on its critical command, control, and communications infrastructure as the prelude to a full-scale attack aimed at neutralizing its nuclear capabilities and choose to strike first. “It is worth considering,” Miller and Fontaine concluded, “how even a very limited attack or incident could set both sides on a slippery slope to rapid escalation.”[10](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote10)

What makes the insertion of latent malware in an adversary’s NC3 systems so dangerous is that it may not even need to be activated to increase the risk of nuclear escalation. If a nuclear-armed state comes to believe that its critical systems are infested with enemy malware, its leaders might not trust the information provided by its early-warning systems in a crisis and might misconstrue the nature of an enemy attack, leading them to overreact and possibly launch their nuclear weapons out of fear they are at risk of a preemptive strike.

“The uncertainty caused by the unique character of a cyber threat could jeopardize the credibility of the nuclear deterrent and undermine strategic stability in ways that advances in nuclear and conventional weapons do not,” Page O. Stoutland and Samantha Pitts-Kiefer wrote in 2018 paper for the Nuclear Threat Initiative. “[T]he introduction of a flaw or malicious code into nuclear weapons through the supply chain that compromises the effectiveness of those weapons could lead to a lack of confidence in the nuclear deterrent,” undermining strategic stability.[11](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote11) Without confidence in the reliability of its nuclear weapons infrastructure, a nuclear-armed state may misinterpret confusing signals from its early-warning systems and, fearing the worst, launch its own nuclear weapons rather than lose them to an enemy’s first strike. This makes the scenario proffered in the 2018 NPR report, of a nuclear response to an enemy cyberattack, that much more alarming.

### 1AC---Solvency

#### Plan: The United States federal government should substantially increase prohibitions on private sector conduct that is more restrictive of competition than reasonably necessary to enable creation of information technology standards.

#### The plan requires SSO’s to administer reasonable action to prohibit ex post opportunism---that strengthens FRAND effectiveness while enabling SEP holders to capture appropriate royalties---which is the best competition-innovation balance.

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)

3. Application of the Basic Legal Principles

The antitrust principle is straightforward: industry-wide collaboration through SSOs to establish procompetitive standards is permitted only if it is no more restrictive of competition than reasonably necessary to enable creation of the standards. When standard setting predictably creates technology monopolies that, if unrestrained, will enable anticompetitive ex post opportunism that would otherwise not occur, an SSO that does not take effective measures to pre- vent or minimize such ex post opportunism engages in conduct that is more restrictive of competition than necessary. In that case, the SSO and, in appropriate cases, its members, may well violate Section 1 of the Sherman Act.

Under this principle, SSO procedures and FRAND rules should be evaluated based on whether they lead to reasonable SEP royalties, using the competitive ex ante licensing standard discussed above, which has been adopted by the courts in patent law. Put differently, FRAND rules should be evaluated based on their ability to prevent SEP holders from obtaining more than the ex ante value of their technology from implementers.

This limitation would not prevent a SEP holder from proﬁting, perhaps greatly, from participating in the SSO and having its patented technology included in the standard. The SEP holder continues to be rewarded for its technology because the inclusion of its technology in the standard can still greatly increase the volume of licensing opportunities available to the SEP holder.

Whether a particular set of FRAND rules are sufficiently effective in preventing ex post opportunism will depend on the particular circumstances. The procedural unfolding of the case will also depend upon the circumstances. As a general matter, the case would probably be structured as an ordinary Rule of Reason case.82

First, the plaintiff would have to demonstrate harm to competition as a result of the collaboration of the SSO’s members, many of which compete with one another. In this case, the harm to competition would stem from the ability of the SEP holder to exercise monopoly power by obtaining royalties in excess of the competitive, ex ante level. The decision to include patented technologies in the standard would be the allegedly unlawful agreement. Notably, the court need not determine what a FRAND royalty is; it would suffice to determine that market power has been created or exercised, and that existing SSO rules and policies were not adequate to prevent the competitive harm. The defendant, which could be the SSO or perhaps one or more SSO members, would win at this point if the plaintiff failed to show harm to competition. If might fail if the standard faces substantial competition and the court concludes that the SEP holder therefore does not have market power or if the SSO’s rules and policies are found to be effective in preventing ex post opportunism, even if the plaintiff or even the court thinks that other rules and policies would be preferable.

Second, if the plaintiff makes the requisite showing of harm to competition, the defendant(s) would then have to show some procompetitive justiﬁcation— in this case, the beneﬁts of the standard. These two initial steps should be straightforward.

Third, if as is likely the defendant is able to show a procompetitive justiﬁcation, the plaintiff would have to show that the SSO could have used available, reasonable alternatives to realize the efficiency beneﬁts with less or none of the competitive harms. The plaintiff might identify reasonable alternatives that would have led to a different standard, based on including unpatented technology in the standard or perhaps involving fewer SEPs or fewer owners of SEPs, which would be less subject to patent holdup. More likely, the plaintiff could suggest alternative SSO rules that would not change the standard, but would reduce the likelihood or extent of ex post opportunism. For example, the plaintiff might suggest more rigorous FRAND-type rules, such as rules that set forth more precise principles on which FRAND royalties are to be determined and the circumstances under which SEP holders might seek injunctions.

Fourth, the burden would then shift to the defendant(s) to show that the beneﬁts of the standard could not have been realized if the SSO had adopted any of the proffered alternatives or that those alternatives were unrealistic.83 The plaintiff would be entitled to judgment if the court concludes that those beneﬁts could have been realized with less competitive harm if the SSO had adopted the standard with different IPR rules or policies.

Our overall sense, based on experience and the empirical literature, is that the extant FRAND rules are generally useful, but tend to be inadequate because they are imprecise and leave unresolved such critical issues as (a) the meaning of a reasonable royalty, even conceptually; (b) the meaning of “non-discriminatory;” (c) to whom licenses must be offered; and (d) under what circumstances may a SEP holder obtain an injunction.84 These imprecise FRAND commitments are therefore not sufficient to adequately prevent ex post opportunism. The recent revisions to IEEE’s FRAND policy represent a signiﬁcant step in the right direction, but even this advance leaves important questions unanswered.85 If FRAND rules are inadequate in these ways, litigation involving extant FRAND rules would likely be resolved only at the ﬁnal, fourth step. The defendant would be able to demonstrate the beneﬁts created by the standard; the plaintiff would be able to demonstrate the creation of market power and that other reasonable and practical rules or policies would ameliorate the problem. The case would thus turn on whether the defendant is able to demonstrate that signiﬁcant beneﬁts associated with standardization could not have been realized if the SSO had adopted those other rules or policies.

The court would have available a variety of possible remedies if the plaintiff prevails. Implementers that paid supracompetitive royalties or were unlawfully excluded in whole or in part from product markets as a result of the inadequate FRAND policies would be entitled to damages and, in some cases, to treble damages.86 If the unlawful SSO conduct is regarded as the collective action of the SSO and its members, which is likely to be the case in most instances, SSO members would be jointly and severally liable for the damages. Forward-looking injunctive relief aimed at restoring competition would need to be fashioned to the requirements of the individual case. For example, a court could order the SSO to adopt a new rule or policy proposed by the plaintiff. If the court is reluctant to take on that governance role, it might give the SSO a period of time—maybe ninety days—to develop a rule, subject to the court’s ultimate approval, which would adequately ameliorate the competitive problem created by the SSO. Alternatively or in addition, the court might order the parties to attempt to negotiate a rule or policy on which they can agree. And, depending on the circumstances, the court might order SEP holders, including at least those that were defendants in the case, to comply with the new SSO rules and policies.

#### Threatening antitrust liability lures SSO’s into adopting best practices.

Lemley & Shapiro 13, \*Mark Lemley is the William H. Neukom Professor at Stanford Law School and a partner at Durie Tangri LLP; \*Carl Shapiro is the Transamerica Professor of Business Strategy at the Haas School of Business, University of California at Berkeley and a Senior Consultant at Charles River Associates; (2013, “A SIMPLE APPROACH TO SETTING REASONABLE ROYALTIES FOR STANDARD-ESSENTIAL PATENTS”, (https://faculty.haas.berkeley.edu/shapiro/frand.pdf)

Under our approach, many of these issues should become moot, since the patentee cannot obtain an injunction (or transfer the patent to someone who can) against a willing licensee, and since competitors are not involved in jointly setting the reasonable royalty rate. If SSOs set clear, reasonable rules following the best practices we recommend, and parties follow those rules, there should be little or no need for antitrust to intervene. Indeed, even the risk of non-disclosure of a patent is lessened, since the patentee has committed to license its essential patents whether or not it discloses them. For the most part, the rules we have described are self-executing, meaning that even if a party tries to break the rules set by the SSO there still may be no need for antitrust to intervene. Thus, we suggest that parties who abide by these procedures—patentees, implementers, and the SSOs themselves—should be immune from antitrust liability for activities that merely follow those rules.107 They have entered into an arrangement that is on balance good for competition, one that allows patentees to receive reasonable royalties but prevents holdup and reduces the risk of monopolization by trickery.

The fact that antitrust remains a last resort available when SSOs don’t follow best practices may have two practical benefits, however. First, under our approach the promise of avoiding the risk of antitrust liability will be a powerful incentive for both SSOs and patent owners to adopt the best practices we propose. Second, the risk of antitrust liability may be relevant when an individual patentee wants to adopt best practices but the SSO governing the standard has not yet done so. We propose that a patentee that unilaterally commits to the FRAND procedures we describe here should be immune from antitrust liability for following these procedures.108 A patentee’s unilateral binding commitment to arbitration could be enforced whether or not it was elicited by an SSO. Thus, just as the prospect of antitrust immunity might lure SSOs to adopt best practices, it might also lure patentees to implement those practices even if the SSO has not done so. Given the large number of standard-essential patents based on preexisting standards,109 and given that SSOs tend to update their IP rules rather slowly,110 this is not a small matter.

#### Only antitrust enforcement creates a consumer-action feature that counterbalances SSO’s conspiratorial incentives---private action fails.

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.

#### Patent holdup is real and necessitates intervention, even if it can’t be systemically proven.

Contreras 19, \*Jorge Contreras, Professor, University of Utah S.J. Quinney College of Law; (2019, “MUCH ADO ABOUT HOLD-UP”, <https://www.illinoislawreview.org/wp-content/uploads/2019/08/Contreras.pdf>)

III. CAN WE PLEASE STOP SEARCHING FOR SYSTEMIC HOLD-UP?

It is not the purpose of this article to critique the data or methodologies used by researchers who claim that there is no evidence of systemic hold-up. Though questions remain, the data presented in the cited studies finding no empirical evidence of systemic hold-up present plausible descriptions of current markets for products such as smart phones and other connected technology devices. Instead, this critique is directed at the core assumption that runs through each of these studies: that a lack of evidence of systemic hold-up means that hold-up does not represent a threat that justifies policy intervention. In this Part, I argue that, notwithstanding the findings of these studies, patent hold-up in standardized product markets may indeed be a threat that merits preventative policy measures, but that those measures should be directed toward the prevention of well-understood and actionable forms of anticompetitive conduct rather than the economic phenomenon of hold-up.

A. The Absence of Systemic Hold-Up Does Not Mean that Hold-Up Does Not Occur

In a 2017 article, Galetovic and Haber utilize an extended analogy drawn from the field of Mayan archeology to make the point that scholars sometimes ignore the facts in front of them in order to cling to pre-formed (and empirically unsupported) beliefs.92 In this analogical tradition, I will use a hypothetical from public health epidemiology to illustrate a related point. Let us consider the often fatal and highly contagious viral infection Ebola. U.S. public health officials, aware of the dangerous effects of Ebola, might propose the implementation of prophylactic measures to prevent the spread of Ebola in the United States. Such measures might include early detection systems at U.S. hospitals, a network of Ebola experts ready to investigate suspected cases, and potential vaccines for particularly vulnerable populations. All of these measures, of course, would come at a cost. Those opposing the incurrence of this cost might argue that such measures are unjustified because there is no empirical evidence that Ebola is a problem in the U.S. After all, there are no documented outbreaks of the disease, and the only reported cases have been sporadic and linked to other factors (such as health workers returning from abroad). In fact, both lifespan and overall health in the United States have been improving steadily over the past several decades. Most declines in population health can be traced to causes such as tobacco use, poor dietary choices, lack of exercise and the like, but not to Ebola. Thus, because there is no evidence that Ebola outbreaks have occurred in the United States nor any linkage between decreased health and Ebola, and because the overall health of the United States population continues to improve, there is no justification for preventative measures to stop Ebola outbreaks in the United States.

This reasoning is, of course, fallacious and, in the case of a disease like Ebola, dangerously so. In the field of public health, prophylactic measures are often taken before a health risk affects a significant portion of the population. This is the reason for prophylactic measures in the first place. In the field of public health, it is widely recognized that risks arising from any number of environmental and pathogenic sources can be assessed based on laboratory analysis and test cases, without population-level epidemiological data. In fact, once population level data for such outbreaks is available, it is often too late: an epidemic has broken out and millions are at risk. Luckily, it is doubtful that public health officials would apply the fallacious reasoning outlined above to important public health decisions.

Curiously, however, this “Ebola fallacy” has taken root in the debate over patent hold-up. As discussed above, the purported lack of empirical evidence of system-wide patent hold-up is used as a justification for abandoning or forestalling policy interventions aimed at reducing the risk of hold-up. Because hold-up has not been detected at a systemic level, so the argument goes, it must not be a problem. Therefore, measures designed to prevent hold-up from occurring must be the result of gratuitous or over-zealous policy making. The logical fallacies in this argument should be apparent.

In fact, there are numerous examples of anticompetitive conduct by individual firms in markets that are not otherwise overrun by anticompetitive behavior. For example, in 2009, the Federal Trade Commission brought an action against pharmaceutical manufacturer Solvay and a group of generic drug manufacturers for violating Section 5 of the FTC Act by entering into an arrangement whereby the generic manufacturers agreed not to challenge Solvay’s patent on its AndroGel product and not to market their generic versions of AndroGel, in exchange for a significant payment by Solvay to each of the generic manufacturers (a so-called “pay for delay” scheme).94 The Supreme Court held in 2013 that such conduct was actionable and reversed the Eleventh Circuit’s dismissal of the FTC’s claim.95 Yet even in 2009, the year in which the FTC brought its action, of the 68 agreements settling patent disputes filed by pharmaceutical manufacturers with the FTC,96 the FTC estimated that only 19 of these (28%) were potential pay for delay agreements; and by 2014, the year after the Actavis decision, only 21 out of 160 such agreements (13%) were deemed by the FTC likely to represent illegal pay for delay schemes.97 Thus, while pharmaceutical industry patent settlements have attracted significant attention as potentially anticompetitive arrangements, most such settlements do not merit investigation by the FTC.98

An even more telling example is found in the area of mergers and acquisitions. During fiscal year 2016, a total of 1,832 merger and acquisition transactions were reported to the FTC and DOJ under the Hart-Scott-Rodino Antitrust Improvements Act.99 Of these, the FTC challenged only twenty-two (1.2%). 100 Thus, while some anticompetitive mergers may exist, the vast majority are not anticompetitive.101 But the absence of market-wide anticompetitive conduct in the area of mergers and acquisitions hardly excuses the handful of transactions that do present antitrust risks, nor does it suggest that mergers should not be subject to governmental monitoring and, when merited, enforcement.

B. Protective Measures May Already Be Working to Reduce Hold-Up

Another important factor that should be considered regarding the purported lack of empirical evidence of systemic hold-up is the effect that existing policy measures have already had in reducing hold-up. As noted above, the threat of patent hold-up was a primary motivating factor for many SDOs to adopt policies requiring the disclosure and licensing of SEPs. These policies have been in place for decades. In the United States, the first such policy was adopted in 1959 by the American Standards Association (the predecessor to today’s American National Standards Institute (ANSI).102 Today, every one of the more than 200 ANSI-accredited developers of American National Standards must adhere to ANSI’s essential requirements, including the adoption of such a licensing policy for SEPs. Similar policies have existed in European and international standards organizations since at least the 1980s.103 These policies, which were developed by SDOs in large part to reduce the likelihood of hold-up within standard-setting systems, have had several decades to work, and it is likely that the lack of observed hold-up in some studies can be attributed to the successful operation of these policies.

Similarly, antitrust and competition enforcement agencies in the U.S. and Europe have been aware of the potential for hold-up connected with standardization for many years. Accordingly, they have brought enforcement actions when it has been alleged that hold-up behavior has resulted in a violation of the antitrust laws. High-profile enforcement actions against patent holders such as Rambus, 104 Google 105 and Qualcomm106 send powerful deterrent signals to the market and warn others not to engage in similar behavior lest they, too, become the subject of agency enforcement. Like SDO policies, it is likely that the general market awareness of agency interest in standard-setting and hold-up has, to a degree, limited the amount of hold-up that is actually attempted in the marketplace, thereby limiting the direct evidence of hold-up as a systemic problem.

But do the deterrent effects of SDO and agency efforts to reduce hold-up signify that hold-up is not a problem? Certainly not. To reach such a conclusion would be perverse: akin to claiming that burglary is not a problem in a neighborhood that experiences reduced burglary rates after it has implemented an active neighborhood watch program and enhanced policing.

C. Indicia of Healthy Markets do not Prove the Absence of Anticompetitive Conduct

As noted above, one of the principal arguments advanced by commentators seeking to refute the “hold-up theory” is that markets for telecommunications products, namely smart phones, are robust – evidenced by increasing product functionality, decreasing consumer prices and rapid innovation -- and that this degree of robustness indicates that hold-up cannot be a problem in these markets.107 If hold-up were a problem in these markets, they reason, we would see product stagnation, stable (but high) prices, and a lack of competition – features associated with classic examples of hold-up in markets for products such as natural resources and agricultural goods.108

But this argument relies on a false syllogism: hold-up results in market dysfunction; if a market functions well, then it cannot be subject to hold-up. The weaknesses in this argument are multifold. First, hold-up may exist in individual instances without sufficient weight to affect overall market characteristics, particularly in a large global market such as mobile telecommunications. Thus hold-up may exist, even in a market that outwardly appears to be functioning well. Second, there is no valid counterfactual to use to compare the health and robustness of the market for mobile telecommunications products.109 Other consumer electronics devices, such as televisions and DVD players, do not compare well with mobile telecommunications devices, which have taken on a unique character in the modern networked economy. Thus, observing the strength of the market fails to answer the critical questions “compared to what?” and how much stronger the market might be (through more product diversity, functionality, price reduction) without hold-up?

A simple historical illustration is useful in this context. During the decade leading up to the enactment of the Sherman Antitrust Act of 1890, several major U.S. commodity markets (e.g., steel, salt, petroleum, coal, sugar, lead, and others) came under intense scrutiny for a variety of allegedly anticompetitive industrial arrangements. One might have argued that these markets, had they been subject to the sorts of anticompetitive collusion that the Sherman Act sought to address, should have seen reductions of output and increases in price. Yet, between 1880 and 1890, U.S. output of salt, petroleum, steel, and coal all increased significantly, and prices of steel, sugar and lead all dropped significantly.110 Do these positive market indicia demonstrate that the subject markets were not subject to anticompetitive collusion, and that the Sherman Act was not necessary? Certainly, investigations of these industries revealed significant cartel behavior. I would suggest that few commentators today would argue that the coal, steel, sugar and other major industrial producers of the late nineteenth century were innocent of collusive and anticompetitive conduct, or that the Sherman Act was not a necessary and beneficial measure for the U.S. economy.111 Yet, had we relied solely on the positive characteristics exhibited by these markets as proof that anticompetitive conduct did not exist, then perhaps the Sherman Act never would have been enacted.

By the same token, the fact that global markets for standardized products such as computers and smart phones appear to be thriving does not itself refute the possibility of hold-up nor the existence of anticompetitive conduct in these markets. Nor does it allow regulators and policy makers to drop their guard or cease to monitor these important industries.