

American University Washington College of Law

## Digital Commons @ American University Washington College of Law

---

Articles in Law Reviews & Other Academic Journals

Scholarship & Research

---

5-2020

### Of Monopolies and Monocultures: The Intersection of Patents and National Security

Charles Duan

Follow this and additional works at: [https://digitalcommons.wcl.american.edu/facsch\\_lawrev](https://digitalcommons.wcl.american.edu/facsch_lawrev)



Part of the [Intellectual Property Law Commons](#), [Internet Law Commons](#), and the [National Security Law Commons](#)

---

## OF MONOPOLIES AND MONOCULTURES: THE INTERSECTION OF PATENTS AND NATIONAL SECURITY

*By Charles Duan*<sup>1</sup>

*Recent conversations about patent policy are increasingly incorporating themes of national security. In particular, the national security dimensions of “races” against technological superpowers such as China, in fields such as artificial intelligence (AI), fifth-generation (5G) mobile communications networks, and quantum computing, has given rise to a national dialogue on spurring domestic innovation, a dialogue into which patents naturally fit. As a result, national security has made a notable appearance in recent key patent policy situations, including the patent subject matter eligibility hearings in the Senate, the Apple–Qualcomm–Federal Trade Commission litigation over patents and antitrust, and the Verizon–Huawei patent licensing dispute. Many of these situations have given rise to an intuitively attractive though simplistic argument: If national security depends on rapid innovation and patents encourage innovation, then stronger patent protection enhances national security.*

*This Article challenges this logic on the relationship between patents and national security, in particular by considering that relationship from the lens of competition. It first turns to history, reviewing several instances in which patent protection has clashed with national security interests. These historical instances, which include pre–World War I torpedo development, the birth of the aviation industry, and post-9/11 bioterrorism responses, demonstrate how the competition-suppressing effects of aggressive patent*

---

<sup>1</sup> Copyright 2019–2020 Charles Duan. Director of Technology and Innovation Policy, R Street Institute, Washington, D.C. This Article represents the author’s individual views and does not necessarily reflect the views of other scholars at the R Street Institute. The author would like to thank Jim Baker, John Bergmayer, Wayne Brough, Walter Evans, L. Zachary Graves, Joshua Landau, Alexandra Moss, Christina Pesavento, Abby Rives, Paul Rosenzweig, Brian Scarpelli, Charlotte Slaiman, Tom Struble, Daniel Takash, Kathryn Waldron, Caleb Watney, K. William Watson, Rachel Wolbers, and several attorneys involved in the litigation discussed below, for their insights that contributed to the author’s understanding of the subject matter, as well as the staff of the Library of Congress. The author would also like to thank the editors of the *Santa Clara High Technology Law Journal* for their excellent suggestions and revisions to this article. Portions of this article were previously submitted in a federal agency comment a submitted statement to a congressional hearing, and an *amicus curiae* brief. See Public Interest Submission of the R Street Institute et al., *In re Certain Mobile Elec. Devices*, 83 Fed. Reg. 64875 (Int’l Trade Comm’n Feb. 6, 2019) (Inv. No. 337-TA-1065), available at <https://www.rstreet.org/wp-content/uploads/2019/02/comments-itc-1065-qva-long.pdf>; 5G: *National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation: Hearing Before the S. Comm. on the Judiciary*, 116th Cong. (2019) (submitted statement of Charles Duan, R Street Institute), available at <https://www.rstreet.org/wp-content/uploads/2019/05/testimony-iot-cybersecurity-2.pdf>; Brief of the R Street Institute as Amicus Curiae in Support of Plaintiff–Appellee, *Fed. Trade Comm’n v. Qualcomm Inc.*, No. 19-16122 (9th Cir. Nov. 28, 2019).

*assertion can diminish national security. Second, this Article considers the effects of diminished competition on cybersecurity, a critical component of modern national security. Economic research shows that competition can enhance cybersecurity, and thus patent-based limits on competition can weaken cybersecurity, both by generating economic incentives to make more secure products and by preventing the formation of technology “monocultures.” These historical and contemporary competition considerations thus lend to policy that balance patent incentives and the value of competition to drive forward security-sensitive technological development.*

## CONTENTS

INTRODUCTION.....	372
I. FACETS OF THE CURRENT DEBATE .....	374
A. <i>The Race to 5G (and AI, and Quantum Computing)</i> .....	374
B. <i>Patent Eligibility of Artificial Intelligence</i> .....	377
C. <i>Qualcomm</i> .....	380
1. The Broadcom Takeover Attempt .....	380
2. The International Trade Commission .....	381
3. The Federal Trade Commission .....	383
D. <i>Verizon and Huawei</i> .....	385
II. PATENTS AND NATIONAL SECURITY IN HISTORY .....	387
A. <i>Pre-World War I Torpedo Development</i> .....	388
B. <i>Aviation and the Wright Brothers</i> .....	390
C. <i>Bioterrorism in the Wake of September 11</i> .....	392
III. COMPETITION AND CYBERSECURITY .....	394
A. <i>Cybersecurity as Competitive Value-Add</i> .....	395
B. <i>Vulnerabilities of “Monocultures”</i> .....	396
IV. LESSONS AND POLICY DIRECTIONS .....	399
A. <i>Anticompetitive Patent Licensing</i> .....	399
B. <i>Prizes, Grants, and Other Incentives for Innovation</i> .....	401
C. <i>Economic Protectionism Versus Enhanced Competition</i> .....	402
D. <i>Protecting the Government Itself: The 2018 NDAA</i> .....	403
CONCLUSION .....	405

## INTRODUCTION

It was certainly an odd thing for the Department of Justice attorney arguing for the United States to appear before the Ninth Circuit to tell the appellate judges that a federal agency was wrong.<sup>2</sup> This was what happened in a Federal Trade Commission enforcement action against Qualcomm Inc., a semiconductor technology company.<sup>3</sup> As a substantial holder of patents on mobile communications technologies and also a leading manufacturer of chips used in that same industry, the FTC charged Qualcomm with anticompetitive conduct; the district court agreed and enjoined Qualcomm from certain patent licensing practices.<sup>4</sup> It was that award of injunctive relief which led the Antitrust Division of the Department of Justice to oppose its administrative counterpart, arguing among other things that the injunction had been improvidently granted in view of the public interest.<sup>5</sup>

Yet as unexpected as the executive branch infighting alone might have been, the grounds for the Justice Department's objection was perhaps unexpected as well. In justifying how the public interest disfavored a remedy on patent licensing, the department reached to a rationale that ordinarily would seem to have nothing to do with patents: national security.<sup>6</sup> By limiting Qualcomm's ability to license its patents, the department argued, the injunction would result in "diminishment of Qualcomm's competitiveness" and thus "could harm U.S. national security."<sup>7</sup>

The Department of Justice has not been alone in drawing a tie between patent policy and national security. Recently, this tie has come up in multiple discussions of patent policy, ranging from hearings on patent subject matter eligibility to patent adjudication before the U.S. International Trade Commission.<sup>8</sup> In those contexts, the Justice Department and many others have advanced a seemingly simple logical argument on how patents implicate national security. It is generally accepted that American national security depends on rapid innovation in certain security-sensitive technologies, such as artificial intelligence and telecommunications.<sup>9</sup> It is also generally accepted that patent protection, being a valuable right granted to inventors, provides an

---

<sup>2</sup> See Oral argument at 18:13, *Qualcomm*, No. 19-16122 (9th Cir. Feb. 13, 2020), [https://www.ca9.uscourts.gov/media/view\\_video.php?pk\\_vid=0000017078](https://www.ca9.uscourts.gov/media/view_video.php?pk_vid=0000017078) (Rawlinson, J.) ("We have two parts of the government here today; that's really . . . interesting.").

<sup>3</sup> See generally *id.*

<sup>4</sup> Fed. Trade Comm'n v. *Qualcomm Inc.*, 411 F. Supp. 3d 658, 820–24 (N.D. Cal. May 21, 2019), *appeal filed*, No. 19-16122 (9th Cir. argued Feb. 13, 2020).

<sup>5</sup> See Brief of the United States of America as Amicus Curiae in Support of Appellant and Vacatur at 29–34, *Qualcomm*, No. 19-16122 (Aug. 30, 2019), Doc. No. 86 [hereinafter *Qualcomm DOJ Amicus Brief*].

<sup>6</sup> See *id.* at 6, 32.

<sup>7</sup> *Id.* at 32; see *infra* notes 74–87.

<sup>8</sup> See generally *infra* Part I (summarizing recent developments relating to patents and national security).

<sup>9</sup> See *infra* notes 18–28.

economic stimulus for innovation.<sup>10</sup> Therefore, maintaining patent protection or even strengthening it ought to further national security; limiting patent rights would conversely “harm U.S. national security” as the Justice Department put it.<sup>11</sup>

This syllogistic equating of patent protection and national security, though perhaps initially attractive, appears on closer inspection to be overly simplistic. The purpose of this Article is to challenge this line of reasoning, showing that patent rights, and in particular unbridled assertion of patents, can impair and repeatedly has impaired national security interests. It reaches this conclusion by considering patents and national security through the lens of competition. Patents by definition suppress competition to some degree,<sup>12</sup> so insofar as competition can enhance national security in certain ways, patents can diminish national security when used or licensed in particularly aggressive ways. To establish the relationship between patents and national security, then, this Article also contemplates how competition relates to national security.

The Article proceeds as follows. Part II reviews how patent policy has recently intersected with national security. It first explains the primary basis for relating innovation policy generally with national security, namely ongoing technological “races” in security-sensitive technologies. It then discusses recent events that have given rise to interest in and arguments over how patent law and policy can affect national security interests, particularly those relating to the aforementioned technology races, and identifies the appearance of the syllogistic argument that patent protection uniformly increases national security.

The remainder of the Article interrogates the syllogistic argument, primarily on two fronts. Part II takes a historical perspective, considering three past anecdotes in which patents have run headlong into national security.<sup>13</sup> While each of the three examples—torpedo development prior to World War I, patent licensing in early aviation, and bioterrorism threats following the September 11th attacks—offers unique insights and lessons (plus an unexpected factoid on *The Sound of Music*<sup>14</sup>), the common thread is that aggressive assertion and licensing of patents, by creating an environment devoid of competition, can stymie important government interests in national defense and security. Part III considers cybersecurity, which is closely tied to

---

<sup>10</sup> See, e.g., *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 480 (1974) (“The patent laws promote this progress by offering a right of exclusion for a limited period as an incentive to inventors to risk the often enormous costs in terms of time, research, and development.”).

<sup>11</sup> Qualcomm DOJ Amicus Brief, *supra* note 5, at 32.

<sup>12</sup> See, e.g., *Lear, Inc. v. Adkins*, 395 U.S. 653, 663 (1969) (“[T]he grant of monopoly power to a patent owner constituted a limited exception to the general federal policy favoring free competition.”).

<sup>13</sup> See *infra* Part II.

<sup>14</sup> See *infra* Part II.A.

national security.<sup>15</sup> Reviewing economic and computer science research, Part III identifies two reasons why competition enhances cybersecurity: Competition encourages firms to improve cybersecurity as a market-driven value-add, and it prevents the formation of single-vendor “monocultures” of technology that have been shown to be especially susceptible to cyberattacks.

Tying any policy field to national security is consequential, because “to securitize an activity or state-of-affairs is to present it as an urgent, imminent, extensive, and existential threat” to the nation at large, thereby justifying “extraordinary responses” that “typically involve bending rules of normal governance.”<sup>16</sup> That is no less true for patent policy: The risk of overly simplistic approach to how patents affect national security could easily be to justify unwarranted expansions of patent protection that could end up undermining the very object sought to be achieved. Accordingly, Part IV offers policy recommendations on how best to address the more nuanced relationship between patents and national security, especially in view of effects on competition.<sup>17</sup>

#### I. FACETS OF THE CURRENT DEBATE

National security is increasingly a component of debates over patent and competition policy. This section describes several contexts in which national security has come up in this debate.

##### A. *The Race to 5G (and AI, and Quantum Computing)*

The backdrop to many of the ties between national security and patent policy has been a number of technology “races” with foreign nations, most notably China. In recent years, China has made significant strides toward positioning itself as a leader in a number of important future technologies.<sup>18</sup> The government’s 2015 report *Made in China 2025* identified several key technology fields, including pharmaceuticals, aerospace, information technology, and robotics, in which the Chinese government intended to make strategic pushes through policy and funding.<sup>19</sup>

<sup>15</sup> See *infra* Part III.

<sup>16</sup> Helen Nissenbaum, *Where Computer Security Meets National Security*, 7 ETHICS & INFO. TECH. 61, 66, 69 (2005).

<sup>17</sup> See *infra* Part IV.

<sup>18</sup> See, e.g., ANDRÉS ORTEGA, THE U.S.–CHINA RACE AND THE FATE OF TRANSATLANTIC RELATIONS, PART I: TECH, VALUES, AND COMPETITION 4–7 (2020), <https://www.csis.org/analysis/us-china-race-and-fate-transatlantic-relations>.

<sup>19</sup> See STATE COUNCIL OF THE P.R.C., MADE IN CHINA 2025, § 3.6, at 22–27 (IoT One trans., 2015), <http://www.cittadellascienza.it/cina/wp-content/uploads/2017/02/IoT-ONE-Made-in-China-2025.pdf>; Scott Kennedy, *Critical Questions: Made in China 2025*, CTR. FOR STRATEGIC & INT’L STUD. (June 1, 2015), <https://www.csis.org/analysis/made-china-2025>.

At least two of these technology areas have raised the eyebrows of national security experts: 5G and artificial intelligence.<sup>20</sup> The former, which relates to new (5th-Generation) wireless telecommunications protocols under development,<sup>21</sup> has led to conversations about the “Race to 5G” between the United States and China.<sup>22</sup> While the concept of a “race” is obviously metaphorical—there is no defined finish line, among other things—there certainly are national security concerns arising from 5G development.<sup>23</sup> Because the technology enables a vastly larger and different class of devices to enter the wireless ecosystem, 5G presents new issues of cybersecurity and also potentially far-reaching military applications.<sup>24</sup> Furthermore, the protocols of 5G systems are set in international multistakeholder standard-setting consortia, meaning that the nation who has the lead in developing aspects of 5G technology will have an advantage during the standard-setting process.<sup>25</sup> It is for these reasons that national security experts warn that “the United States and its allies cannot fall substantially behind China in 5G implementation.”<sup>26</sup>

Artificial intelligence has given rise to similar concerns, with experts worrying that China’s massive investments in AI research could lead the country to possess superior computer software technologies, possibly tied to military applications.<sup>27</sup> And lest it be thought that the United States is in only two races, commentators have also pointed to a race for “quantum supremacy,” relating to an advanced computing technology with the potential

<sup>20</sup> See, e.g., Nitin Dahad, *US, China Vying for AI and 5G Supremacy*, EE TIMES (Apr. 19, 2019), <https://www.eetimes.com/us-china-vying-for-ai-and-5g-supremacy/>.

<sup>21</sup> See Jeffrey G. Andrews et al., *What Will 5G Be?*, 32 IEEE J. ON SELECTED AREAS COMM. 1065, 1075 (2014).

<sup>22</sup> See Stu Woo, *In the Race to Dominate 5G, China Sprints Ahead*, WALL ST. J. (Sept. 7, 2019), <https://www.wsj.com/articles/in-the-race-to-dominate-5g-china-has-an-edge-11567828888>; Doug Brake, *Economic Competitiveness and National Security Dynamics in the Race for 5G between the United States and China* 11–12, in 46 TPRC: RES. CONF. ON COMM. INFO. & INTERNET POL’Y (2018), available at <https://ssrn.com/abstract=3142229>. But see, e.g., Kevin Werbach, *Opinion: The “Race to 5G” Is a Myth*, CNN BUS. (Feb. 3, 2020), <https://www.cnn.com/2020/02/03/perspectives/5g-disruption/index.html> (disputing that 5G development is a “race”).

<sup>23</sup> See Brake, *supra* note 22, at 20.

<sup>24</sup> See Jim Baker, *5G Networks Must Be Secure and Reliable*, LAWFARE (Mar. 13, 2019), <https://www.lawfareblog.com/5g-networks-must-be-secure-and-reliable>.

<sup>25</sup> See Brake, *supra* note 22, at 17–18; Eli Greenbaum, *5G, Standard-Setting, and National Security*, HARV. NAT’L SECURITY J. ONLINE (July 3, 2018), <https://harvardnsj.org/2018/07/5g-standard-setting-and-national-security/>.

<sup>26</sup> Baker, *supra* note 24.

<sup>27</sup> See GREGORY C. ALLEN, UNDERSTANDING CHINA’S AI STRATEGY: CLUES TO CHINESE STRATEGIC THINKING ON ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY 3–4 (2019), <https://nsiteam.com/social/wp-content/uploads/2019/05/CNAS-Understanding-Chinas-AI-Strategy-Gregory-C.-Allen-FINAL-2.15.19.pdf>; NAT’L SEC. COMM’N ON ARTIFICIAL INTELLIGENCE, INTERIM REPORT 11, 17–18 (2019), <https://www.epic.org/foia/epic-v-ai-commission/AI-Commission-Interim-Report-Nov-2019.pdf>.



for breaking modern encryption.<sup>28</sup> The ongoing competition for technical superiority between the United States and China, in multiple fields, thus has important national security implications.

Amidst this dialogue has been a concern about whether national security concerns are masking domestic economic protectionism. When the Trump Administration instituted tariffs on steel and aluminum imports, for example, the proffered justification was that steel and aluminum manufacturing implicated national security because domestic steel industries were necessary for fabricating weapons, manufacturing military vehicles such as aircraft and ships, and building critical infrastructure.<sup>29</sup> But commentators noted that the justification was questionable in view of the facts, and wondered whether the tariffs were in fact no more than a license for existing domestic incumbents to keep their prices high.<sup>30</sup>

China has also been accused of “intellectual property theft,” referring to industrial espionage practices, and “forced technology transfer,” in which the government requires disclosure of trade-secret technologies as a condition for doing business in China.<sup>31</sup> These practices do not relate to patents, nor could they given that patents are published for anyone to read.<sup>32</sup> While there are no

<sup>28</sup> See Arthur Herman, *The Quantum Computing Threat to American Security*, WALL ST. J. (Nov. 10, 2019), <https://www.wsj.com/articles/the-quantum-computing-threat-to-american-security-11573411715>.

<sup>29</sup> See OFFICE OF TECH. EVALUATION, U.S. DEP’T OF COMMERCE, THE EFFECT OF IMPORTS OF STEEL ON THE NATIONAL SECURITY: AN INVESTIGATION CONDUCTED UNDER SECTION 2323 OF THE TRADE EXPANSION ACT OF 1962, AS AMENDED 23–24 (2018), [https://www.commerce.gov/sites/default/files/the\\_effect\\_of\\_imports\\_of\\_steel\\_on\\_the\\_national\\_security\\_-\\_with\\_redactions\\_-\\_20180111.pdf](https://www.commerce.gov/sites/default/files/the_effect_of_imports_of_steel_on_the_national_security_-_with_redactions_-_20180111.pdf); OFFICE OF TECH. EVALUATION, U.S. DEP’T OF COMMERCE, THE EFFECT OF IMPORTS OF ALUMINUM ON THE NATIONAL SECURITY: AN INVESTIGATION CONDUCTED UNDER SECTION 2323 OF THE TRADE EXPANSION ACT OF 1962, AS AMENDED 23–39 (2018), [https://www.commerce.gov/sites/default/files/the\\_effect\\_of\\_imports\\_of\\_aluminum\\_on\\_the\\_national\\_security\\_-\\_with\\_redactions\\_-\\_20180117.pdf](https://www.commerce.gov/sites/default/files/the_effect_of_imports_of_aluminum_on_the_national_security_-_with_redactions_-_20180117.pdf).

<sup>30</sup> See Clark Packard & Megan Reiss, *Steel Protectionism Won’t Protect National Security*, LAWFARE (Jan. 12, 2018), <https://www.lawfareblog.com/steel-protectionism-wont-protect-national-security>; Menzie Chinn, *What Is the National Security Rationale for Steel, Aluminum and Automobile Protection?*, ECONOFACT (June 6, 2018), <https://econofact.org/what-is-the-national-security-rationale-for-steel-aluminum-and-automobile-protection>.

<sup>31</sup> See, e.g., U.S. TRADE REPRESENTATIVE, FINDINGS OF THE INVESTIGATION INTO CHINA’S ACTS, POLICIES, AND PRACTICES RELATED TO TECHNOLOGY TRANSFER, INTELLECTUAL PROPERTY, AND INNOVATION UNDER SECTION 301 OF THE TRADE ACT OF 1974, at 17–18 (2018), <https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF> (reviewing these practices); Jyh-An Lee, *Shifting IP Battlegrounds in the U.S.—China Trade War*, 43 COLUM. J.L. & ARTS 147, 183–84 (2020) (noting that U.S. focus on Chinese intellectual property practices has “shifted” from counterfeiting to “acquiring IP and confidential information”).

<sup>32</sup> See Lee, *supra* note 31, at 183–84; cf. Debora Halbert, *Intellectual Property Theft and National Security: Agendas and Assumptions*, 32 INFO. SOC’Y 256, 260 (2016) (noting government’s and commentators’ failure to “delve into the technical differences between intellectual property regimes such as copyright, patent, trademark, and trade secrets” when considering intellectual property “theft”). There are some, even within the government, that have classified among China’s misappropriations of U.S. technologies the practice of “systematic, large-scale, open-source collection operations” including “analyzing patents.” See WHITE HOUSE OFFICE OF TRADE & MFG. POLICY, HOW CHINA’S ECONOMIC AGGRESSION THREATENS THE TECHNOLOGIES AND INTELLECTUAL PROPERTY OF THE UNITED STATES AND THE WORLD 13 (June 2018), <https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL->

doubts that national security implications exist for espionage, they are distinct from any patent-specific concerns and thus not the subject of this Article.

In large part, concerns over China's relevant innovation practices in 5G, AI, and other such fields stem from China's practice of choosing "national champions," which include firms that the state heavily subsidizes or even partially controls in order to bolster the chances that those firms succeed in the global market.<sup>33</sup> In the telecommunications space, for example, Chinese phone manufacturer Huawei is largely understood to be heavily funded and managed by the state.<sup>34</sup> That China and other nations sponsor these national champions in technologies has forced American companies and policymakers to think carefully about how to respond to this form of state-backed competition.<sup>35</sup>

### B. Patent Eligibility of Artificial Intelligence

The national security concerns about these technology races lend to an easy, if simplistic, argument: If patents provide incentives for innovation, then increasing patent protection will increase national security by propelling innovation in technologies such as artificial intelligence and 5G. That argument has been made multiple times recently, most notably in the context of legislation over patentable subject matter eligibility.

Eligibility is one of the requirements for an invention to be patentable in the United States. Under 35 U.S.C. § 101, a patent may issue for "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof."<sup>36</sup> While that language standing alone appears expansive, courts have interpreted that statute to embody several historical restrictions on the patentability of certain subject matter.<sup>37</sup> In

---

China-Technology-Report-6.18.18-PDF.pdf. The notion that impropriety lies in the mere act of reading published patents is difficult to reconcile with the very nature of patents as published. Cf. Invention Secrecy Act of 1951, 35 U.S.C. § 181 (enabling government to "withhold the publication" of a patent or application if "publication or disclosure by the publication of an application or by the grant of a patent on an invention in which the Government has a property interest might, in the opinion of the head of the interested Government agency, be detrimental to the national security").

<sup>33</sup> See, e.g., U.S. TRADE REPRESENTATIVE, *supra* note 31, at 19; NAT'L SEC. COMM'N ON ARTIFICIAL INTELLIGENCE, *supra* note 27, at 21; Dhruva Jaishankar, *From the iPhone to Huawei: The New Geopolitics of Technology*, LAWFARE (Aug. 1, 2019), <https://www.lawfareblog.com/iphone-huawei-new-geopolitics-technology>.

<sup>34</sup> See Ellen Nakashima, *U.S. Pushes Hard for a Ban on Huawei in Europe, but the Firm's 5G Prices Are Nearly Irresistible*, WASH. POST (May 29, 2019), [https://www.washingtonpost.com/world/national-security/for-huawei-the-5g-play-is-in-europe--and-the-us-is-pushing-hard-for-a-ban-there/2019/05/28/582a8ff6-78d4-11e9-b7ae-390de4259661\\_story.html](https://www.washingtonpost.com/world/national-security/for-huawei-the-5g-play-is-in-europe--and-the-us-is-pushing-hard-for-a-ban-there/2019/05/28/582a8ff6-78d4-11e9-b7ae-390de4259661_story.html) ("The company . . . has a silent partner: the Chinese government. Huawei gets hundreds of millions of dollars in annual subsidies . . .").

<sup>35</sup> See Sharon Poczter et al., *How to Compete Against the New Breed of National Champions*, MIT SLOAN MGMT. REV. 5–6 (May 30, 2018), [http://ilp.mit.edu/media/news\\_articles/smr/2018/59431.pdf](http://ilp.mit.edu/media/news_articles/smr/2018/59431.pdf).

<sup>36</sup> 35 U.S.C. § 101 (2018).

<sup>37</sup> See, e.g., *Gottschalk v. Benson*, 409 U.S. 63, 67–69 (1972) (citing *Le Roy v. Tatham*, 55 U.S. (14 How.) 156, 175 (1852); *O'Reilly v. Morse*, 56 U.S. (15 How.) 62, 111–13 (1853)).

particular, the Supreme Court has held that “laws of nature, natural phenomena, and abstract ideas” are not eligible for patenting under § 101.<sup>38</sup> In recent decisions, this eligibility limit has been held to prevent patenting of isolated human genetic sequences,<sup>39</sup> diagnostic test correlations,<sup>40</sup> financial investment strategies,<sup>41</sup> and computerized methods for financial transactions.<sup>42</sup>

Discontent and uncertainty over these decisions limiting the patent eligibility of a variety of technologies led to calls for legislation to revise § 101, ultimately resulting in the Intellectual Property Subcommittee of the Senate Judiciary Committee holding a series of hearings on the subject.<sup>43</sup> Much of the criticism of § 101 related to the diagnostic testing and life sciences sector,<sup>44</sup> but because one of the Supreme Court’s decisions related to the eligibility of computer software,<sup>45</sup> many commentators feared that the patent eligibility bar had been set too high for emerging computer technologies such as artificial intelligence.<sup>46</sup>

It was this criticism of § 101’s impact on artificial intelligence and other computer technologies that gave rise to arguments about national security: Those calling for amending the patent eligibility requirements contended that if Congress did not amend § 101, then the United States would fall behind in

<sup>38</sup> *Diamond v. Diehr*, 450 U.S. 175, 185 (1981).

<sup>39</sup> *See Ass’n for Molecular Pathology v. Myriad Genetics, Inc.*, 569 U.S. 576, 591 (2013).

<sup>40</sup> *See Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 79–80 (2012).

<sup>41</sup> *See Bilski v. Kappos*, 561 U.S. 593, 609 (2010).

<sup>42</sup> *See Alice Corp. Pty. Ltd. v. CLS Bank Int’l*, 134 S. Ct. 2347, 2359–60 (2014).

<sup>43</sup> *See The State of Patent Eligibility in America: Part I: Hearing Before the Subcomm. on Intellectual Property of the S. Comm. on the Judiciary*, 116th Cong. (June 4, 2019), <https://www.judiciary.senate.gov/meetings/the-state-of-patent-eligibility-in-america-part-i>; *The State of Patent Eligibility in America: Part II: Hearing Before the Subcomm. on Intellectual Property of the S. Comm. on the Judiciary*, 116th Cong. (June 5, 2019), <https://www.judiciary.senate.gov/meetings/the-state-of-patent-eligibility-in-america-part-ii>; *The State of Patent Eligibility in America: Part III: Hearing Before the Subcomm. on Intellectual Property of the S. Comm. on the Judiciary*, 116th Cong. (June 11, 2019), <https://www.judiciary.senate.gov/meetings/the-state-of-patent-eligibility-in-america-part-iii>.

<sup>44</sup> *See, e.g., Ariosa Diagnostics, Inc. v. Sequenom, Inc.*, 809 F.3d 1282, 1285 (Fed. Cir. 2015) (denial of rehearing en banc) (Lourie, J., concurring) (“It is said that the whole category of diagnostic claims is at risk. It is also said that a crisis of patent law and medical innovation may be upon us, and there seems to be some truth in that concern.”); Warren D. Woessner & Robin A. Chadwick, *Section 101: What’s Left to Patent in the Life Sciences after Myriad, Mayo, and Alice*, 101 J. PAT. & TRADEMARK OFF. SOC’Y 121, 158–59 (2019).

<sup>45</sup> *See Alice*, 134 S. Ct. at 2359–60.

<sup>46</sup> *See, e.g., Andrei Iancu, The Current State of Innovation within the U.S. Legal System—Views on Evolving Protection for Intellectual Property Rights in the United States from the USPTO and the Courts*, 101 J. PAT. & TRADEMARK OFF. SOC’Y 11, 13 (2019) (disputing § 101 jurisprudence in view of the “Fourth Industrial Revolution” when “scientists and engineers are working at forever faster rates to make advancements in artificial intelligence (AI), robotics, biotechnology, autonomous vehicles, quantum computing, and so much more”); *Smart Sys. Innovations v. Chi. Transit Auth.*, 873 F.3d 1364, 1378 (Fed. Cir. 2017) (“And the danger of getting the answers to [patent eligibility] questions wrong is greatest for some of today’s most important inventions in computing, medical diagnostics, artificial intelligence, the Internet of Things, and robotics, among other things.”), *quoted in The State of Patent Eligibility in America: Part III*, *supra* note 43 (testimony of Manny Schecter, IBM Corp.).

security-sensitive technologies.<sup>47</sup> U.S. Patent and Trademark Office Director Andrei Iancu, for example, has remarked that the United States is “in a globally-competitive innovation race,” so “to maintain our technological leadership,” the nation “must be careful not to decide that the automation that is at the heart of the technologies of the future is somehow not eligible for patenting.”<sup>48</sup>

Former Director of the U.S. Patent and Trademark Office David Kappos has been particularly vocal on the tie between patent eligibility and national security. In congressional testimony, he has argued that the Supreme Court’s eligibility jurisprudence “poses not only a threat to our global economic leadership, but also to our national security,” citing artificial intelligence, quantum computing, and 5G as examples.<sup>49</sup> Kappos’s testimony before the Subcommittee on Intellectual Property similarly remarked that the “current constricted approach to Section 101 is undermining investment in technologies Congress and the Administration consider critical to national security,” citing to data suggesting that the United States had rejected patent applications under § 101 that had been allowed for patenting in China and Europe.<sup>50</sup> (The accuracy of that data has been questioned.<sup>51</sup>)

To be sure, national security appears to be just a talking point with respect to patent eligibility, rather than the motivating factor for any patent policy reform. But national security is a powerful talking point,<sup>52</sup> and its

<sup>47</sup>See, e.g., Brian Pomper, *The Real US Patent “Crisis,”* THE HILL (Dec. 9, 2019), <https://thehill.com/blogs/congress-blog/technology/473757-the-real-us-patent-crisis> (“Restoring clear patent rights will be essential to maintaining a strong and healthy U.S. innovation ecosystem. That, in turn, will help U.S. innovators keep up with the fierce international competition to develop the technologies so critical to the future of U.S. national security, including artificial intelligence, advanced computing and 5G.”).

<sup>48</sup>Iancu, *supra* note 46, at 13.

<sup>49</sup>David J. Kappos, *National Security Consequences of U.S. Patent (In)eligibility*, MORNING CONSULT (Nov. 4, 2019), <https://morningconsult.com/opinions/national-security-consequences-of-u-s-patent-ineligibility/>.

<sup>50</sup>See *The State of Patent Eligibility in America: Part I: Hearing Before the Subcomm. on Intellectual Property of the S. Comm. on the Judiciary*, 116th Cong. (June 4, 2019), <https://www.judiciary.senate.gov/imo/media/doc/Kappos%20Testimony.pdf> (oral testimony of David J. Kappos, Partner, Cravath, Swaine & Moore LLP).

<sup>51</sup>The data set, collected by Kappos and Robert Sachs, was analyzed in Kevin Madigan & Adam Mossoff, *Turning Told Into Lead: How Patent Eligibility Doctrine Is Undermining U.S. Leadership in Innovation*, 24 GEO. MASON L. REV. 939, 941 n.10 (2017). However, of the exemplary patents discussed in that article, see *id.* at 957–58 fig.4, a subsequent analysis found that only one was rejected solely under § 101, and three were not facing a § 101 rejection at all. See Josh Landau, “Gold Into Lead” Article Focuses on Pyrite Patents, PAT. PROGRESS (June 13, 2018), <https://www.patentprogress.org/2018/06/12/gold-into-lead-article-focuses-on-pyrite-patents/>.

<sup>52</sup>*Cf.* MAROUF HASIAN JR. ET AL., THE RHETORICAL INVENTION OF AMERICA’S NATIONAL SECURITY STATE 5 (2015) (“The formation and maintenance of America’s national security state needs to be viewed as a rhetorical accomplishment, something that involves the active participation of everyone from the president, to military members, to Hollywood directors, and many more in between.”).

appearance in dialogues over patent policy suggests a need for careful thought about how exactly patent policy and national security intersect.

### C. *Qualcomm*

Among the instances where patent policy has intersected with national security concerns, one name repeatedly appears: Qualcomm Inc., a San Diego-based semiconductor design firm. The company itself may not be a household name, but its products are in practically every household, with between 43% and 52% market share in the baseband processor chips found in every cell phone.<sup>53</sup> Commentators have raised national security in the context of Qualcomm on too many occasions to count, but at least three specific policy actions brought the issue to the fore.

#### 1. The Broadcom Takeover Attempt

In late 2017, Singapore-based Broadcom Ltd. announced its intention to buy out Qualcomm for \$105 billion.<sup>54</sup> Being a foreign acquisition of a U.S. firm, review of the proposed transaction fell to the Committee on Foreign Investment in the United States, or CFIUS, an interagency committee of the federal government.<sup>55</sup> CFIUS ultimately recommended against Broadcom's acquisition attempt, and President Trump ratified that decision in an order prohibiting the acquisition.<sup>56</sup>

Although the takeover itself did not necessarily implicate either patents or national security, CFIUS deigned to make it so. In its letter opposing the acquisition, CFIUS began by describing Qualcomm as a “global leader in the development and commercialization of foundational technologies” for mobile communications.<sup>57</sup> Qualcomm's “dominant role” offered “significant

<sup>53</sup> See Strategy Analytics, Inc., *Strategy Analytics: Q1 2018 Baseband Market Share: Samsung LSI Overtakes MediaTek*, BUSINESSWIRE (July 31, 2018), <https://www.businesswire.com/news/home/20180731005614/en/Strategy-Analytics-Q1-2018-Baseband-Market-Share> [hereinafter Strategy Analytics 2018] (52%); Strategy Analytics, Inc., *2Q 2019 Baseband Market Share: Qualcomm and Samsung Emerge as Early 5G Contenders*, BUSINESSWIRE (Oct. 15, 2019), <https://www.businesswire.com/news/home/20191015005732/en/Strategy-Analytics---2Q-2019-Baseband-Market> [hereinafter Strategy Analytics 2019] (43%). See also Fed. Trade Comm'n v. Qualcomm Inc., 411 F. Supp. 3d at 690, 695 (finding that Qualcomm “has owned a dominant share” and “possessed monopoly power” in certain mobile phone chip markets).

<sup>54</sup> See Michael J. de la Merced, *Broadcom Targets Qualcomm in Biggest Technology Deal Ever*, N.Y. TIMES, Nov. 7, 2017, at B1.

<sup>55</sup> See Diane Bartz, *Exclusive: Secretive U.S. Security Panel Discussing Broadcom's Qualcomm Bid*, REUTERS (Mar. 6, 2018), <https://www.reuters.com/article/us-qualcomm-m-a-broadcom-exclusive-idUSKCN1GB09V>.

<sup>56</sup> See Order Regarding the Proposed Takeover of Qualcomm Incorporated by Broadcom Limited, 83 Fed. Reg. 11631, sec. 2(a) (Mar. 15, 2018); Cecilia Kang & Alan Rappeport, *Trump Blocks Broadcom's Bid for Qualcomm*, N.Y. TIMES (Mar. 12, 2018), <https://www.nytimes.com/2018/03/12/technology/trump-broadcom-qualcomm-merger.html>.

<sup>57</sup> Letter from Aimen N. Mir, Dep't of the Treasury, to Mark Plotkin & Theodore Kassinger, *CFIUS Case 18-036: Broadcom Limited (Singapore)/Qualcomm Incorporated*, U.S. DEP'T OF THE TREASURY 2 (Mar. 5, 2018), available at <http://online.wsj.com/public/resources/documents/cfiusletter.pdf> [hereinafter CFIUS Letter].

confidence” with respect to national security, according to CFIUS.<sup>58</sup> Going on to note that “Qualcomm’s current business model is based upon licensing of patented Qualcomm technologies,” CFIUS concluded that any changes to that patent licensing model “could result in a weakening of Qualcomm’s technological leadership in a manner that is detrimental to U.S. national security.”<sup>59</sup>

Put another way, national security depends, in CFIUS’s view, on Qualcomm’s patent licensing business remaining undisturbed. Indeed, practitioners noted the unusual nature of this CFIUS action: “While CFIUS and the president have rejected numerous deals in the past based on the acquisition of intelligence capabilities or sensitive technology by a foreign buyer, this is the first deal rejected by a president based squarely on the market role and competitiveness of the U.S. company.”<sup>60</sup> Others have said that the decision “canonized the San Diego company as a sort of national champion.”<sup>61</sup> This remarkable turn of events shows how patents, competition policy, and national security can unexpectedly cross paths.

## 2. The International Trade Commission

In 2017, Apple Inc. filed suit against Qualcomm on the grounds of anticompetitive behavior.<sup>62</sup> In response, Qualcomm brought multiple actions against Apple for patent infringement, including two actions before the U.S. International Trade Commission, or ITC, a federal trade agency that has the power to exclude importation of products deemed to infringe patents.<sup>63</sup>

Again, although national security was not the issue before the agency, it nevertheless became a paramount concern in the ITC. Prior to issuing an exclusion order that would prevent importation of products deemed to infringe

---

<sup>58</sup> *Id.*

<sup>59</sup> *Id.* at 3.

<sup>60</sup> David Mortlock et al., *The President and CFIUS Expand Exercise of CFIUS Authority by Blocking Broadcom Takeover of Qualcomm*, WILLKIE FARR & GALLAGHER LLP 2 (Mar. 14, 2018), [https://www.willkie.com/media/Files/Publications/2018/03/The\\_President\\_and\\_CFIUS\\_Expand\\_Exercise\\_of\\_CFIUS\\_Authority.pdf](https://www.willkie.com/media/Files/Publications/2018/03/The_President_and_CFIUS_Expand_Exercise_of_CFIUS_Authority.pdf).

<sup>61</sup> Ted Greenwald et al., *Rejection of Qualcomm–Broadcom Deal Followed Monthslong Strategy*, WALL ST. J. (Mar. 14, 2018), <https://www.wsj.com/articles/rejection-of-qualcomm-broadcom-deal-followed-monthslong-strategy-1520986563>; accord Claude Barfield, *So Qualcomm Is a National Champion. Now What?*, AM. ENTERPRISE INST. (Mar. 23, 2018), <https://www.aei.org/technology-and-innovation/so-qualcomm-is-a-national-champion-now-what/>.

<sup>62</sup> See *Apple Inc. v. Qualcomm Inc.*, No. 3:17-cv-108, slip op. at 5 (S.D. Cal. Sept. 7, 2017) (order denying anti-suit injunction).

<sup>63</sup> See *In re Certain Mobile Elec. Devices*, 82 Fed. Reg. 37899 (Int’l Trade Comm’n Aug. 14, 2017); *In re Certain Mobile Elec. Devices*, 83 Fed. Reg. 834 (Int’l Trade Comm’n Jan. 8, 2018). The former investigation concluded with a finding of no infringement, see *In re Certain Mobile Elec. Devices*, 84 Fed. Reg. 12292 (Int’l Trade Comm’n Apr. 1, 2019); the latter settled, see *In re Certain Mobile Elec. Devices*, 84 Fed. Reg. 44330 (Int’l Trade Comm’n Aug. 23, 2019). See generally Shara Tibken, *Apple and Qualcomm Settle Licensing Dispute Amid Trial’s Opening Arguments*, CNET (Apr. 16, 2019), <https://www.cnet.com/news/apple-and-qualcomm-settle-licensing-dispute-during-opening-arguments/> (describing other litigation between Apple and Qualcomm).

a patent, the ITC must weigh whether exclusion would be in the “public interest,” based on a list of four statutory factors.<sup>64</sup> Apple argued, and the administrative law judge at the ITC agreed, that exclusion would not be in the public interest because of “a real and palpable likelihood the National Security interests will be jeopardized.”<sup>65</sup> At the time, the ITC judge found, Qualcomm and Intel were the only two market suppliers of “premium baseband chip sets,” the component that smartphones use to communicate with cell towers.<sup>66</sup> Furthermore, Intel was found to be likely to exit the premium baseband chip market if the ITC were to issue an exclusion order against Apple.<sup>67</sup> Applying a straightforward “[t]wo suppliers [are] better than one monopolist” theory of market competition,<sup>68</sup> the administrative law judge found that an exclusion order that would have the effect of strangling Intel’s whole market share would leave the United States undercompetitive in 5G technology—a risk to “the preservation of a strong U.S. presence in the development of 5G and thus the national security of the United States.”<sup>69</sup>

The ITC granted review of the administrative law judge’s determination and invited public comment on the public interest question,<sup>70</sup> which sparked a wave of debate over patents and national security. Supporters of the decision (of which this Article’s author was one) largely agreed with the administrative law judge’s findings.<sup>71</sup> Critics of the decision, on the other hand, followed a line similar to CFIUS’s reasoning, contending that because Qualcomm was the dominant U.S. firm, any harm to its status as leader (e.g., competition from Intel) would diminish America’s 5G capacity and thus harm national

---

<sup>64</sup> The statutory factors are “the public health and welfare, competitive conditions in the United States economy, the production of like or directly competitive articles in the United States, and United States consumers.” Tariff Act of 1930 § 337(d)(1), 19 U.S.C. § 1337 (2018) (as amended); see Colleen V. Chien & Mark A. Lemley, *Patent Holdup, the ITC, and the Public Interest*, 98 CORNELL L. REV. 1, 19–28 (2012) (discussing ITC’s application of the public interest factors).

<sup>65</sup> See *In re Certain Mobile Elec. Devices*, No. 337-TA-1065, at 196 (Int’l Trade Comm’n Sept. 28, 2018) (initial determination and recommended determination), available at <https://www.patentprogress.org/wp-content/uploads/2019/01/ALJ-Pender-ITC-Initial-Final-Decision-337-TA-1065.pdf>.

<sup>66</sup> See *id.* at 190.

<sup>67</sup> See *id.* at 191.

<sup>68</sup> See *id.* at 192.

<sup>69</sup> See *id.* at 195.

<sup>70</sup> See *In re Certain Mobile Elec. Devices*, 83 Fed. Reg. 64875 (Int’l Trade Comm’n Dec. 18, 2018).

<sup>71</sup> See Public Interest Statement of the R Street Institute et al., *In re Certain Mobile Elec. Devices*, 83 Fed. Reg. 54138 (Int’l Trade Comm’n Oct. 26, 2018) (Inv. No. 337-TA-1065); Public Interest Submission of the R Street Institute et al., *Certain Mobile Elec. Devices*, 83 Fed. Reg. 64875 (Feb. 6, 2019) (Inv. No. 337-TA-1065), available at <https://www.rstreet.org/wp-content/uploads/2019/02/comments-itc-1065-qva-long.pdf>; Bill Watson, *Abusing Trade Law to Ban iPhones Is Not in the Public Interest*, THE HILL (Dec. 9, 2018), <https://thehill.com/opinion/technology/420425-abusing-trade-law-to-ban-iphones-is-not-in-the-public-interest>; Ashley Durkin-Rixey, *Patents and the Public Interest: What Does the ITC Ruling Against Qualcomm Really Mean?*, ACT — APP ASS’N (Dec. 3, 2018), <https://actonline.org/2018/12/03/patents-and-the-public-interest-what-does-the-itc-ruling-against-qualcomm-really-mean/>.

security.<sup>72</sup> Although the ITC ultimately decided the investigation on other grounds and Qualcomm settled with Apple shortly thereafter,<sup>73</sup> the ITC had flushed out a vigorous debate over how patent policy and competition affect national security.

### 3. The Federal Trade Commission

Apple was not the only one to charge Qualcomm with anticompetitive behavior: A spate of foreign competition agencies had charged Qualcomm with demanding excessive royalties in violation of competition laws across the mid-2010s.<sup>74</sup> In 2017, their American counterpart, the Federal Trade Commission, followed suit by bringing an action against Qualcomm in the Northern District of California for violations of the Sherman and FTC Acts.<sup>75</sup> The premise of *Federal Trade Commission v. Qualcomm Inc.* (“*FTC v. Qualcomm*”) was reasonably straightforward: Qualcomm held a market-dominant position over certain mobile communications chips, and it leveraged that monopoly to overcharge phone manufacturers for patent licenses through a “no license–no chips” policy under which Qualcomm would refuse to sell chips without first reaching a licensing deal on a bundle of patents.<sup>76</sup>

Yet again, national security was not an issue in the district court litigation; “national security” is not mentioned once in the district court’s 233-page findings of fact and conclusions of law.<sup>77</sup> Once the trial had completed in the FTC’s favor, however, national security did come to the fore. After an appeal had been docketed in the Ninth Circuit, Qualcomm moved for a stay of

<sup>72</sup> See, e.g., James Edwards, *ITC’s Chance to Restore Reason and the Public Interest in the Qualcomm v. Apple Case*, IPWATCHDOG (Nov. 8, 2018), <https://www.ipwatchdog.com/2018/11/08/its-chance-to-restore-reason-and-the-public-interest-in-the-qualcomm-apple-case/id=103078/> (citing CFIUS Letter, *supra* note 57). The other argument that these critics raised was that application of the public interest to deny an exclusion order “is tantamount to abrogating the rule of law,” on the theory that the statute requires exclusion as a remedy to patent infringement. *Id.* That reasoning is puzzling given that statute specifically names the public interest factors as reasons why “articles should not be excluded from entry.” Tariff Act of 1930 § 337(d)(1), 19 U.S.C. § 1337 (2018) (as amended).

<sup>73</sup> See *In re Certain Mobile Elec. Devices*, 84 Fed. Reg. 12292 (Int’l Trade Comm’n Apr. 1, 2019); Don Clark & Daisuke Wakabayashi, *Apple and Qualcomm Settle All Disputes Worldwide*, N.Y. TIMES, Apr. 17, 2019, at B1.

<sup>74</sup> See Se Young Lee, *South Korea Fines Qualcomm \$854 Million for Violating Competition Laws*, REUTERS (Dec. 28, 2016), <https://www.reuters.com/article/us-qualcomm-antitrust-idUSKBN14H062> (noting investigations in South Korea, China, the European Union, and Taiwan); *Fed. Trade Comm’n v. Qualcomm Inc.*, 411 F. Supp. 3d at 807, 675–76 (also noting Japan), *appeal filed*, No. 19-16122 (9th Cir. argued Feb. 13, 2020).

<sup>75</sup> See *Fed. Trade Comm’n*, 411 F. Supp. 3d at 669.

<sup>76</sup> See Complaint for Equitable Relief ¶¶ 2–7, at 2–3, *Fed. Trade Comm’n*, 411 F. Supp. 3d 658 (No. 5:17-cv-00220-LHK), [https://www.ftc.gov/system/files/documents/cases/170117qualcomm\\_redacted\\_complaint.pdf](https://www.ftc.gov/system/files/documents/cases/170117qualcomm_redacted_complaint.pdf); Timothy B. Lee, *How Qualcomm Shook Down the Cell Phone Industry for Almost 20 Years*, ARS TECHNICA (May 30, 2019), <https://arstechnica.com/tech-policy/2019/05/how-qualcomm-shook-down-the-cell-phone-industry-for-almost-20-years/>.

<sup>77</sup> See generally *Fed. Trade Comm’n*, 411 F. Supp. 3d at 658.



enforcement of the district court judgment,<sup>78</sup> and supporting Qualcomm's motion was a statement of interest from the Antitrust Division of the Department of Justice.<sup>79</sup> The statement of interest itself came as no surprise given DOJ's repeated criticisms of the application of antitrust law to patent holders.<sup>80</sup> But what was unusual was the inclusion of two declarations from officials at the Department of Energy<sup>81</sup> and the Department of Defense.<sup>82</sup> Both essentially recited the same argument: Qualcomm, being the dominant firm in certain markets, was a provider of chips to both departments, and both expressed concern that "it would be impossible to replace Qualcomm's critical role in 5G technology in the short-term," so "[a]ny measure that inappropriately reduces Qualcomm's revenue substantially . . . could harm national security."<sup>83</sup>

In granting Qualcomm's motion, the Ninth Circuit was apparently swayed by these national security arguments. Citing to the DOD and DOE declarations, the motions panel contemplated the possibility "that the injunction threatens national security."<sup>84</sup> While the panel did not indicate whether it agreed with the agencies' positions, it did find the fact that "the government itself is divided about the propriety of the judgment and its impact on the public interest" sufficient to grant the motion to stay execution.<sup>85</sup>

Qualcomm's pre-argument motion was not the last word on national security in the case. Responding to and criticizing the contentions of the Department of Justice and its supporting agencies, former Secretary of Homeland Security Michael Chertoff explained in an op-ed in the *Wall Street Journal* that "the view that a single manufacturer of a product critical national defense should be, in effect, protected from competition" could be "catastrophic" for national security.<sup>86</sup> And at oral argument, the Ninth Circuit panel questioned the attorney for the Department of Justice extensively on the

---

<sup>78</sup> See Qualcomm's Motion for Partial Stay of Injunction Pending Appeal, Fed. Trade Comm'n v. Qualcomm Inc., No. 19-16122 (9th Cir. July 8, 2019), Doc. No. 9.

<sup>79</sup> See United States' Statement of Interest Concerning Qualcomm's Motion for Partial Stay of Injunction Pending Appeal, *Qualcomm*, No. 19-16122 (July 16, 2019), Doc. No. 25.

<sup>80</sup> See, e.g., Makan Delrahim, Address at the 19th Annual Berkeley-Stanford Advanced Patent Law Institute: "Telegraph Road": Incentivizing Innovation at the Intersection of Patent and Antitrust Law (Dec. 7, 2018), <https://www.justice.gov/opa/speech/assistant-attorney-general-makan-delrahim-delivers-remarks-19th-annual-berkeley-stanford> ("I have criticized the argument that it ought to be a violation of antitrust law for a holder of a standard-essential patent, or SEP, to exclude competitors from using the technology . . .").

<sup>81</sup> See Declaration of Department of Energy Chief Information Officer Max Everett, *Qualcomm*, No. 19-16122 (July 16, 2019), Doc. No. 25-3 [hereinafter DOE Declaration].

<sup>82</sup> See Declaration of Under Secretary of Defense for Acquisition and Sustainment Ellen M. Lord, *Qualcomm*, No. 19-16122 (July 16, 2019), Doc. No. 25-2 [hereinafter DOD Declaration].

<sup>83</sup> *Id.* ¶ 16, at 7; see DOE Declaration, *supra* note 81, ¶ 10, at 6.

<sup>84</sup> Fed. Trade Comm'n v. Qualcomm Inc., 935 F.3d 752, 756 (9th Cir. Aug. 23, 2019) (per curiam order on motion to stay).

<sup>85</sup> *Id.*

<sup>86</sup> Michael Chertoff, *Qualcomm's Monopoly Imperils National Security*, WALL ST. J., Nov. 25, 2019, at A17.

merits of the Department's national security argument, expressing skepticism where the Department "ha[d]n't offered any market analysis or financial evidence that the injunction would actually harm national security."<sup>87</sup> The *FTC v. Qualcomm* case thus presents a clash of different perspectives on how patents and competition policy affect national security.

#### D. *Verizon and Huawei*

It is difficult to discuss national security and technology policy without mentioning the Chinese telecommunications manufacturer Huawei Technologies.<sup>88</sup> Recent events relating to that company also illuminate the interactions between patents and national security.

Huawei has been a constant focus for national security. As noted above, the company is one of China's "national champions" receiving substantial resources and assistance from the Chinese government.<sup>89</sup> That relationship has led national security experts to raise concerns about whether China can leverage Huawei mobile communications infrastructure equipment for espionage or surveillance purposes, by installing covert backdoors in software for example.<sup>90</sup> The U.S. Department of Commerce has placed Huawei on its "entity list," restricting American firms' ability to do business with Huawei;<sup>91</sup> the company has also been accused of industrial espionage, along the lines of the "IP theft" issues discussed above.<sup>92</sup>

<sup>87</sup> Matthew Renda, *Qualcomm, FTC Spar at 9th Circuit over What Makes a Monopoly*, COURTHOUSE NEWS SERV. (Feb. 13, 2020), <https://www.courthousenews.com/qualcomm-ftc-spar-over-what-makes-a-monopoly-at-ninth-circuit-hearing/> (quoting Murphy, J.).

<sup>88</sup> The company has its own tag on the national security policy blog *Lawfare*, with approximately thirty-five entries between February 2018 and February 2020. See *Huawei – Tags*, LAWFARE, <https://www.lawfareblog.com/tagged/huawei> (last visited Apr. 26, 2020). By contrast, during the same time period, there have been only fifteen entries on that blog tagged for encryption, another major national security policy issue. See *Encryption – Tags*, LAWFARE, <https://www.lawfareblog.com/tagged/encryption> (last visited Apr. 26, 2020).

<sup>89</sup> See Nakashima, *supra* note 34 and accompanying text.

<sup>90</sup> See Bojan Pancevski, *U.S. Officials Say Huawei Can Covertly Access Telecom Networks*, WALL ST. J. (Feb. 11, 2020), <https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256>. But see HUAWEI CYBER SEC. EVALUATION CTR. OVERSIGHT BD., ANNUAL REPORT TO THE NATIONAL SECURITY ADVISER OF THE UNITED KINGDOM § 3.18 (Mar. 2019), [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/790270/HCSEC\\_OversightBoardReport-2019.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf) (finding that risks of Huawei technologies stem from "[p]oor software engineering and cybersecurity processes," not intentional espionage channels as "a result of Chinese state interference"); Lily Hay Newman, *Huawei's Problem Isn't Chinese Backdoors. It's Buggy Software*, WIRED (Mar. 28, 2019), <https://www.wired.com/story/huawei-threat-isnt-backdoors-its-bugs/>.

<sup>91</sup> See Addition of Certain Entities to the Entity List and Revision of Entries on the Entity List, 84 Fed. Reg. 43493, 43495–96 (Bureau of Indus. & Sec., Dep't of Commerce Aug. 21, 2019) (codified at 15 C.F.R. PART 744, SUPPLEMENT 4); 15 C.F.R. § 744.11(a) (requiring a license "to export, reexport, or transfer (in-country) any item subject to the EAR to an entity that is listed on the Entity List").

<sup>92</sup> See Superseding Indictment ¶¶ 8–10, at 3–4, *United States v. Huawei Techs. Co.*, No. 1:18-cr-457 (E.D.N.Y. Feb. 13, 2020) (Doc. No. 126), <https://www.justice.gov/opa/press-release/file/1248961/download>. See also sources cited *supra* notes 31–32 and accompanying text.

As a telecommunications firm, Huawei also is a substantial player in patents. For 5G technology, Huawei leads in the number of patent families declared as essential to the 5G standard, with 3,325 declared families of which 1,337 have at least one granted patent.<sup>93</sup> The company reportedly holds 56,492 active patents worldwide overall,<sup>94</sup> and has already engaged in high-stakes patent litigation worldwide.<sup>95</sup>

Huawei's patent capabilities notably reached American shores in June 2019, when the company initiated demands that Verizon Communications take licenses to over 200 Huawei patents.<sup>96</sup> Negotiations escalated over the following months, until Huawei filed suit against Verizon in early 2020.<sup>97</sup> Huawei was reportedly seeking "more than \$1 billion" in royalties.<sup>98</sup> Reports of these licensing demands led several senators to propose legislation that would block Huawei and like companies from asserting or licensing patents,<sup>99</sup> though those proposals were widely panned by patent practitioners worried that cutting back on the assertion value of patents would devalue patent protection and encourage China into "tit-for-tat restriction on patent enforcement."<sup>100</sup>

<sup>93</sup> See IPLYTICS GMBH, WHO IS LEADING THE 5G PATENT RACE? A PATENT LANDSCAPE ANALYSIS ON DECLARED 5G PATENTS AND 5G STANDARDS CONTRIBUTIONS 5 tbl.1 (2019), [https://www.iptytics.com/wp-content/uploads/2019/01/Who-Leads-the-5G-Patent-Race\\_2019.pdf](https://www.iptytics.com/wp-content/uploads/2019/01/Who-Leads-the-5G-Patent-Race_2019.pdf).

<sup>94</sup> See Susan Decker, *Huawei Has 56,492 Patents and It's Not Afraid to Use Them*, BLOOMBERG (June 14, 2019), <https://www.bloomberg.com/news/articles/2019-06-14/huawei-has-56-492-patents-and-it-s-not-afraid-to-use-them> (citing data from analytics firm).

<sup>95</sup> See, e.g., Takashi Kawakami, *Samsung and Huawei Drop Lawsuits in Latest Smartphone Truce*, NIKKEI ASIAN REV. (May 15, 2019), <https://asia.nikkei.com/Business/Companies/Samsung-and-Huawei-drop-lawsuits-in-latest-smartphone-truce>; Case C-170/13, *Huawei Techs. Co. v. ZTE Corp.*, 2015 E.C.R. 477; *Unwired Planet Int'l Ltd. v. Huawei Techs. Co.*, [2018] EWCA (Civ) 2344 (Eng.), available at <https://www.bailii.org/ew/cases/EWCA/Civ/2018/2344.pdf>.

<sup>96</sup> See Sarah Krouse, *Huawei Presses Verizon to Pay for Patents*, WALL ST. J. (June 12, 2019), <https://www.wsj.com/articles/huawei-presses-verizon-to-pay-for-patents-11560354414>.

<sup>97</sup> See Complaint, *Huawei Techs. Co. v. Verizon Commc'ns, Inc.*, No. 6:20-cv-00090 (W.D. Tex. Feb. 5, 2020), 2020 WL 592355.

<sup>98</sup> David Shepardson, *Huawei Asks Verizon to Pay Over \$1 Billion for Over 230 Patents: source*, REUTERS (June 12, 2019), <https://www.reuters.com/article/us-huawei-tech-verizon-patents-idUSKCN1TD218>; accord Paul Mozur & Edmund Lee, *Huawei Is Said to Demand Patent Fees From Verizon*, N.Y. TIMES (June 12, 2019), <https://www.nytimes.com/2019/06/12/technology/huawei-verizon-patent-license-fees.html> (reporting unnamed sources claiming that "Huawei's claims would exceed \$1 billion in fees").

<sup>99</sup> See Patricia Zengerle, *Senator Rubio Targets Huawei over Patents*, REUTERS (June 18, 2019), <https://www.reuters.com/article/us-huawei-tech-usa-senate-idUSKCN1TI2T3>; 165 CONG. REC. S3573 (daily ed. June 13, 2019) (Senate Amendment 551 introduced by Sen. Rubio); Prevent Abuse of the Legal System Act, S. 2178, 116th Cong. secs. 2(b)–c (July 18, 2019).

<sup>100</sup> Jacob Schindler, *Rubio's Huawei Proposal Should Worry US Tech, Pharma Companies*, IAM MAG. (June 23, 2019), <https://www.iam-media.com/law-policy/rubios-huawei-proposal-should-worry-us-tech-pharma-companies>; see also Kieren McCarthy, *You're Huawei Off Base on This, Rubio: Lawyers Slam US Senator's Bid to Ban Chinese Giant from Filing Patent Lawsuits*, THE REGISTER (June 21, 2019), [https://www.theregister.co.uk/2019/06/21/huawei\\_patents\\_rubio/](https://www.theregister.co.uk/2019/06/21/huawei_patents_rubio/).

Though national security has not so far been the main focus of the Verizon–Huawei patent dispute, that dispute adds an important dimension to the relationship between patents and national security.<sup>101</sup> The arguments in discourse over Qualcomm<sup>102</sup> and Chinese technological races<sup>103</sup> have focused on how patent protection affects *American* firms' activities with respect to national security—whether patents or competition will better encourage American companies to innovate more, for example. But Huawei's assertion of patents suggests that patent protection enables *foreign* firms to affect national security.<sup>104</sup> If foreign companies are able to tie up American firms in years of patent litigation, then the diversion of domestic resources from research and development to legal disputes may interfere with success in technology races for AI and telecommunications. Since international agreements prevent the United States from discriminating between domestic and foreign inventors with respect to patents,<sup>105</sup> the possibility that patents could serve as a tool for foreign competitors to harass American firms is something that national security experts need to consider carefully.

## II. PATENTS AND NATIONAL SECURITY IN HISTORY

While current disputes have brought attention to the interplay between patents and national security, they are not the first time those areas have crossed paths. On multiple occasions throughout history, patent licensing has intersected with national security. In particular, considered below are examples of those intersections that illustrate how aggressive use of patents has left the United States ill-prepared to face contemporary threats. These examples contain important lessons about the relationship among patents, competition, and national security.

To be sure, patents are important incentives for innovation that drive the development of new technologies including those that better protect Americans, and patent-holding inventors are due reasonable compensation for their inventive work. The problems have arisen not from the mere existence

---

<sup>101</sup> See generally Charles Duan, *Do Patents Protect National Security?*, LAWFARE (July 12, 2019), <https://www.lawfareblog.com/do-patents-protect-national-security>.

<sup>102</sup> See *supra* Part I.C.

<sup>103</sup> See *supra* Part I.A.

<sup>104</sup> See also Mike Masnick, *Once Again, China Is About to Use the US's Obsession with "Intellectual Property" Against Us*, TECHDIRT (May 30, 2019), <https://www.techdirt.com/articles/20190521/23373342258/once-again-china-is-about-to-use-uss-obsession-with-intellectual-property-against-us.shtml> (noting Chinese practices of using "patents to block American competitors and to even block US companies in other countries").

<sup>105</sup> See Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, art. 3, para. 1, 1869 U.N.T.S. 299, 302 [hereinafter TRIPS Agreement] ("Each Member shall accord to the nationals of other Members treatment no less favourable than that it accords to its own nationals with regard to the protection of intellectual property . . . ." (footnote omitted)).

of patents, but from their owners' decisions to leverage them to extract as much private value as possible without concern for public consequences.

*A. Pre-World War I Torpedo Development*

The development of the torpedo offers a useful example for the present study because it shows the dangers of the United States being dependent on a single monopoly producer of critical technology.

At the start of the 20th century, it was apparent that naval supremacy was contingent on torpedoes. A 1903 U.S. Naval War College conference report concluded, based on simulations of U.S.–German naval battles, that torpedoes “turn the scale of battle in their favor in a most decided manner” and recommended arming ships with them.<sup>106</sup> This jolted the Navy’s Bureau of Ordnance into accelerating its torpedo development work, and in particular forming a public–private partnership in 1904 with the E.W. Bliss Company and its engineer Frank M. Leavitt to develop and manufacture the then-experimental Bliss–Leavitt torpedo.<sup>107</sup>

Unfortunately, “what was commercially valuable for the Bliss Company was not necessarily militarily valuable for the Navy,” and patent licensing became a focal point of that misalignment.<sup>108</sup> The Bliss Company was a licensee of key patents on the superheater, a technology for torpedo propulsion.<sup>109</sup> Bliss negotiated with the government to license those patents from 1905 through 1912, ultimately dragging the government into litigation through 1920.<sup>110</sup> Nor was the government blameless: It sought its own patent on torpedo stabilization, which further bungled the relationship between Bliss and the government.<sup>111</sup>

Two problems arose, at least in part because of this patent infighting between Bliss and the government. The decades of litigation likely consumed resources from both sides that could otherwise have been put to innovation.<sup>112</sup> Moreover, the patent disputes reflected a larger campaign on the part of Bliss to monopolize the torpedo market at the expense of the U.S. government. In 1906, Bureau head N.E. Mason wrote that “the Bureau has been handicapped by the knowledge that, due to the monopoly held by the company, the Bureau would have to accept the terms offered or get no torpedoes. The Bureau has become convinced that a belief in the helplessness of the Government has

---

<sup>106</sup> KATHERINE C. EPSTEIN, *TORPEDO: INVENTING THE MILITARY-INDUSTRIAL COMPLEX IN THE UNITED STATES AND GREAT BRITAIN* 68–69 (2014).

<sup>107</sup> *See id.* at 69–70.

<sup>108</sup> *Id.* at 73.

<sup>109</sup> *See* E.W. Bliss Co. v. United States, 253 U.S. 187, 188 (1920) [hereinafter *Bliss II*].

<sup>110</sup> *See id.* at 189–90; EPSTEIN, *supra* note 106, at 93–94.

<sup>111</sup> *See* E.W. Bliss Co. v. United States, 248 U.S. 37, 40 (1918) [hereinafter *Bliss I*]; EPSTEIN, *supra* note 106, at 82–83.

<sup>112</sup> *See Bliss I*, 248 U.S. at 40; *Bliss II*, 253 U.S. at 189–90.

influenced the E. W. Bliss Company in its prices, deliveries and workmanship.”<sup>113</sup>

Dependence on an exclusive domestic torpedo innovator would have consequences. Bliss ultimately failed to deliver on its promises for the Bliss–Leavitt torpedo and, by 1907, had to ask the Bureau to reduce the performance minimums in the contract.<sup>114</sup> Mark Bristol of the Naval Torpedo Station connected that failure to the Bliss Company’s efforts at monopolization, lecturing in 1909 that company’s “‘get rich quick’ scheme” had left it “failing to improve the turbine” such that “the Bliss–Leavitt torpedo today is inferior to the Whitehead,” its foreign competitor with close ties to the Austro-Hungarian Empire.<sup>115</sup> His observation is consistent with the general trend of dominant market power diminishing incentives to innovate.<sup>116</sup>

With Bliss unable to make torpedoes up to spec, the Bureau in 1907 found itself forced to turn to those Austrian Whitehead torpedoes, first purchasing them and then licensing the rights to manufacture.<sup>117</sup> Thus, on the eve of World War I, the U.S. Navy was “scarcely equipped to enter the war” and indeed dependent on war technology sourced from an empire that would soon be an enemy.<sup>118</sup>

Besides showing how patent posturing can affect national security, the Bliss–Leavitt torpedo debacle highlights the dangers of American dependence on single-firm supply. In a current environment where the United States government concedes its own dependence on monopoly suppliers such as Qualcomm for security-critical technologies,<sup>119</sup> it should be alarming that a century ago, monopoly in also-critical torpedo technology nearly sunk the Navy.

<sup>113</sup> EPSTEIN, *supra* note 106, at 86 (quoting letter from Mason to the Secretary of the Navy, Oct. 17, 1906).

<sup>114</sup> *See id.* at 88.

<sup>115</sup> *Id.* at 102. The Whitehead factory was based in Fiume (Rijeka), a naval base of the Austro-Hungarian Navy, and the torpedo was developed for the Austrian navy. *See* LAWRENCE SONNENHAUS, *THE NAVAL POLICY OF AUSTRIA-HUNGARY, 1867–1918*, at 47–48 (1994). Robert Whitehead, the torpedo inventor and factory namesake, was also the grandfather of Agathe Whitehead, whose famously Austrian husband was Captain Georg von Trapp. *See* Joan Gearin, *Movie vs. Reality: The Real Story of the Von Trapp Family*, PROLOGUE MAG. (Winter 2005), <https://www.archives.gov/publications/prologue/2005/winter/von-trapps.html>; Alan Wolstencroft, *The Whitehead Story*, 59 MARINER’S MIRROR 345, 347 (1973).

<sup>116</sup> *See infra* notes 183–185.

<sup>117</sup> *See* EPSTEIN, *supra* note 106, at 87 (quoting letters from Bureau head N.E. Mason to the Secretary of the Navy); Naval Service Appropriations Act, ch. 2512, § 1, 34 STAT. 1176, 1180 (1907).

<sup>118</sup> EPSTEIN, *supra* note 106, at 103.

<sup>119</sup> *See, e.g.*, DOD Declaration, *supra* note 82, ¶ 5 (“DoD national security programs . . . rely on continued access to Qualcomm products . . . . Any disruption of supply of Qualcomm products or services to the U.S. Government, or of Qualcomm’s related R&D, even for a short period of time, could have a detrimental impact on national security.”).

### B. Aviation and the Wright Brothers

On the eve of World War I, the United States stood at a stark disadvantage to Europe in the air: The government in 1913 held 6 military airplanes to France's 266, and a federal official lamented that the country had fallen "from first place to last of all the great nations in the air."<sup>120</sup> The root cause of this deficiency was again aggressive patent licensing, in this case instigated by no less than Orville and Wilbur Wright.

The Wright brothers are famous for solving the key lateral-roll problem of aviation;<sup>121</sup> they are infamous for aggressively litigating the resulting patent. Throughout the early 1900s, the Wrights filed multiple suits against their main competitor, airplane manufacturer Glenn Curtiss, in what the newspapers termed the "patent wars."<sup>122</sup> They also sued foreign aviators at American exhibitions, often springing the lawsuits unexpectedly on the aviators or show exhibitors immediately after the shows.<sup>123</sup>

How did airplane patent litigation contribute to America's technological lag? The conventional theory is that the Wrights' patent licensing demands dissuaded American firms from investing in aviation technology,<sup>124</sup> but a handful of dissenting historians reply that substantial investment in aviation was occurring in the United States.<sup>125</sup> Evaluating this disagreement is not straightforward. The dissenters are correct that there was not a total industry holdup, but it is unclear whether investment was nevertheless depressed or was falling behind Europe, where for a variety of reasons patent litigation was

<sup>120</sup> TOM D. CROUCH, *WINGS: A HISTORY OF AVIATION FROM KITES TO THE SPACE AGE* 147 (2003).

<sup>121</sup> See U.S. Patent No. 821,393 (issued May 22, 1906); *Wright Co. v. Herring-Curtiss Co.*, 204 F. 597, 600 (W.D.N.Y. 1913), *aff'd*, 211 F. 654 (2d Cir. 1914) (per curiam).

<sup>122</sup> *End Patent Wars of Aircraft Makers*, N.Y. TIMES, Aug. 7, 1917, at 5; see *Wright Co. v. Herring-Curtiss Co.*, 177 F. 257, 261 (C.C.W.D.N.Y. 1910) (granting preliminary injunction); *Wright Co. v. Herring-Curtiss Co.*, 211 F. 654 (2d Cir. 1914) (per curiam) (final appeal). Upon the Wrights' litigation victory in 1914, Curtiss devised a workaround and the Wrights promptly sued again; that case never went to trial and was ultimately mooted by the creation of an aviation patent pool in 1917. See FRED C. KELLY, *THE WRIGHT BROTHERS* 296 (Dover Publ'ns 1989).

<sup>123</sup> See Herbert A. Johnson, *The Wright Patent Wars and Early American Aviation*, 69 J. AIR L. & COM. 21, 31–33 (2004); *Wright Co. v. Paulhan*, 177 F. 261, 271 (C.C.S.D.N.Y. 1910).

<sup>124</sup> See, e.g., Johnson, *supra* note 123, at 42–43; 1 ALEX ROLAND, *MODEL RESEARCH: THE NATIONAL ADVISORY COMMITTEE FOR AERONAUTICS 1915–1958*, at 38 (1985); Robert P. Merges & Richard R. Nelson, *On the Complex Economics of Patent Scope*, 90 COLUM. L. REV. 839, 890–91 (1990); Scott McCartney, *Wright Brothers' Patent Battle Proved Costly in Aviation Race*, WALL ST. J. (Dec. 17, 2003), <https://www.wsj.com/articles/SB107159573141697200>; Phaedra Hise, *How The Wright Brothers Blew It*, FORBES (Nov. 19, 2003), <https://www.forbes.com/2003/11/19/1119aviation.html>.

<sup>125</sup> See Tom D. Crouch, *Blaming Wilbur and Orville: The Wright Patent Suits and the Growth of American Aeronautics*, in *ATMOSPHERIC FLIGHT IN THE TWENTIETH CENTURY* 290–91 (Peter Galison & Alex Roland eds., 2000); Ron D. Katznelson & John Howells, *The Myth of the Early Aviation Patent Hold-up—How a US Government Monopsony Commandeered Pioneer Airplane Patents*, 24 INDUS. & CORP. CHANGE 1, 11 (2014).

not as prevalent.<sup>126</sup> Furthermore, there is disagreement as to whether the demanded royalties were “almost confiscatory”<sup>127</sup> or not.<sup>128</sup> It is perhaps notable, though, that the demanded royalty is strikingly like Qualcomm’s: The Wright–Martin company demanded 5–10% on gross receipts (not net profits) of finished products (not the smallest salable patent-practicing unit) on all airplane-related products (not just those using the patent) including accessories, instruments, training school tuition, and flight show tickets.<sup>129</sup>

A better explanation of the Wrights’ impact on aviation innovation is found in the economic theory of “knowledge spillovers.” Economists posit that much innovation in and across industries occurs when researchers are in close proximity with each other, such that knowledge can informally “spill over” within the community and particularly within countries.<sup>130</sup> The spillover effect is most prominent when the community contains a diversity of innovators, such that “local competition promotes growth.”<sup>131</sup>

In view of this economic theory, it becomes apparent that a driving cause of the lack of aviation innovation in the United States was a lack of knowledge spillovers stemming from the Wrights’ patent litigation. The result of their suing foreign aviators and enjoining aviation exhibitions was that “all the foreign aviators of note have assured that they will not sign contracts to appear” in the United States while litigation was pending.<sup>132</sup> And the ongoing, bitter litigation between Curtiss and the Wrights meant that two of the most powerful American innovators were essentially out of commission for years.<sup>133</sup> Without a robust influx of experts and technologists, innovation could not occur in the United States at the same rate as in Europe, which by 1910 had outstripped the United States in airplane motor and wing design.<sup>134</sup> Thus, “the Wrights virtually isolated American aviation from knowledge of rapid European improvement of airplane design and manufacture.”<sup>135</sup>

<sup>126</sup> See Johnson, *supra* note 123, at 25; Christine MacLeod, *Reluctant Entrepreneurs: Patents and State Patronage in New Technosciences, Circa 1870–1930*, 103 *ISIS* 328, 337 (2012).

<sup>127</sup> See LAWRENCE GOLDSTONE, *BIRDMEN: THE WRIGHT BROTHERS, GLENN CURTISS, AND THE BATTLE TO CONTROL THE SKIES* 203 (2014).

<sup>128</sup> See Katznelson & Howells, *supra* note 125, at 33–34.

<sup>129</sup> See *Application for License and Form of Agreement of the Wright–Martin Aircraft Corporation*, in 54 CONG. REC. 3238 (1917); cf. *Fed. Trade Comm’n v. Qualcomm Inc.*, 935 F.3d 752, 672–74 (9th Cir. argued Feb. 13, 2020). All this was stacked on top of whatever royalty Curtiss intended to demand. See *Makers Must Buy a Curtiss License*, *N.Y. TIMES*, Dec. 20, 1916, at 14.

<sup>130</sup> See Adam B. Jaffe et al., *Geographic Localization of Knowledge Spillovers as Evidenced by Patent Citations*, 108 Q.J. ECON. 577, 578 (1993).

<sup>131</sup> Edward L. Glaeser et al., *Growth in Cities*, 100 J. POL. ECON. 1126, 1129 (1992).

<sup>132</sup> *Foreign Aviators Shy of Infringement Suits on Aeroplane Patents in America*, *BOSTON SUNDAY GLOBE*, Mar. 13, 1910, at 11; see GOLDSTONE, *supra* note 127, at 200.

<sup>133</sup> See GOLDSTONE, *supra* note 127, at 236 (“For Glenn Curtiss and the Wrights, whose attention was deflected from the shop to either the courtroom or the boardroom, this presented a significant impediment to remaining competitive.”).

<sup>134</sup> See *id.* at 236–37.

<sup>135</sup> Johnson, *supra* note 123, at 31.



Indeed, even one of the dissenting historians appears to support this knowledge spillover issue. “Strenuous competition between a relatively large number of designers and aviators in Europe,” Dr. Tom D. Crouch explains, “led to the exploration of a wide range of configurations, the use of new materials, and improved control systems and power plants.”<sup>136</sup> By contrast, American aviators “had not been tested under the constant pressure to fly higher, faster and farther against a wide range of competitors,” leaving them and American airplane manufacturers “largely committed to the original configuration of the Wright airplane” and with “little incentive to change.”<sup>137</sup> Crouch concludes that the greater prevalence of air shows and exhibitions in Europe drove this competitive pressure toward innovation,<sup>138</sup> but overlooks the fact that the dearth of air shows in the United States was a direct result of patent litigation.

This knowledge spillover problem should cast a long shadow over patent policy. The lesson of the early aviation industry is that a dominant market position, in combination with aggressive patent licensing that keeps a whole industry under the patent holder’s thumb, can deny the United States the advantage of innovative collaborations and knowledge spillovers. Given the extensive control that a handful of patent-holding firms exert over the mobile telecommunications market,<sup>139</sup> one might anticipate parallel consequences in that industry today. And indeed, Qualcomm’s patent litigation arguably contributed to the loss of a key American 5G innovator, Intel.<sup>140</sup> Allowing market concentration to clog the knowledge spillover pathway to innovation could thus deny American superiority in key technologies now, just as it did a century ago.

### C. *Bioterrorism in the Wake of September 11*

Aggressive patent licensing imperiled national security again in 2001 by jeopardizing the ability of the United States to protect the public from threats of bioterrorism. In the wake of the September 11 attacks, there was an immediate and credible threat of a mass attack of weaponized anthrax immune to traditional antibiotics.<sup>141</sup> Defending against this threat required a stockpile of treatments ready to deploy in cities of millions blanketed with airborne

---

<sup>136</sup> Crouch, *supra* note 125, at 292–93.

<sup>137</sup> *Id.* at 292.

<sup>138</sup> *See id.*

<sup>139</sup> *See* Fed. Trade Comm’n v. Qualcomm Inc., 411 F. Supp. 3d 658, 674 (N.D. Cal. 2019).

<sup>140</sup> *See* Chaim Gartenberg, *Intel Says Apple and Qualcomm’s Surprise Settlement Pushed It to Exit Mobile 5G*, THE VERGE (Apr. 25, 2019), <https://www.theverge.com/2019/4/25/18516830/intel-apple-qualcomm-surprise-settlement-pushed-exit-mobile-5g-modems>.

<sup>141</sup> *See Effective Responses to the Threat of Bioterrorism: Hearing Before the Subcomm. on Public Health of the S. Comm. on Health, Education, Labor, and Pensions*, 107th Cong. 5 (Oct. 9, 2001) (statement of Sen. Bill Frist); Elisabeth Bumiller, *Public Health Or Public Relations*, N.Y. TIMES, Oct. 21, 2001, § 4, at 4.

anthrax spores.<sup>142</sup> At the time, only one treatment was approved to treat anthrax: ciprofloxacin, or Cipro, an antibiotic manufactured—and patented—by the pharmaceutical firm Bayer AG.

Two problems arose out of Bayer's patent. First, Bayer's prices for the drug were exceptionally high—35 times the cost of identical generics.<sup>143</sup> Second and more problematic was Bayer's own production capacity. The government estimated it would need a stockpile of 60 days' treatment for 12 million people.<sup>144</sup> Generic manufacturers estimated they could fill that need in 3 months, but Bayer determined that its own factories would require "20 months, working 24 hours a day" to fulfill the requisition.<sup>145</sup> Nevertheless, Bayer refused to permit generics to manufacture the drug.<sup>146</sup>

Bayer's stance left the Bush administration torn between honoring the company's patent and readying for a mass anthrax disaster. On the one hand, the government could have invoked its powers under 28 U.S.C. § 1498 to allow generic entry at the cost of "reasonable and entire compensation."<sup>147</sup> But "breaking" Bayer's patents would have been globally hypocritical in light of the government's arguments that South Africa could not do the same to patents on AIDS treatments.<sup>148</sup> On the other hand, it would have been no less hypocritical for the government to leave the American public unprotected, especially given that it had been giving Cipro to White House staff as of September 11.<sup>149</sup>

The Health and Human Services Department initially avoided invoking § 1498, hoping to negotiate a deal between Bayer and the generic manufacturers.<sup>150</sup> But as political pressure mounted, HHS changed course and prepared to call for legislation circumventing Bayer's patent, forcing Bayer

---

<sup>142</sup> See OFFICE OF TECH. ASSESSMENT, OTA-ISC-559, PROLIFERATION OF WEAPONS OF MASS DESTRUCTION: ASSESSING THE RISKS 54 fig.2-2 (Aug. 1993), <https://ota.fas.org/reports/9341.pdf>.

<sup>143</sup> See Donald G. McNeil Jr., *A Rush for Cipro, and the Global Ripples*, N.Y. TIMES, Oct. 17, 2001, at A1.

<sup>144</sup> See Elisabeth Bumiller, *Administration Won't Allow Generic Versions of Drug*, N.Y. TIMES, Oct. 18, 2001, at B8. Some saw this as an underestimate, including "Representative Bernard Sanders, a Vermont independent who favors a much larger government role in the nation's health system." Keith Bradsher & Edmund L. Andrews, *U.S. Says Bayer Will Cut Cost of Its Anthrax Drug*, N.Y. TIMES, Oct. 24, 2001, at B7.

<sup>145</sup> Bumiller, *supra* note 144.

<sup>146</sup> See *id.*

<sup>147</sup> 28 U.S.C. § 1498(a) (1998).

<sup>148</sup> See McNeil Jr., *supra* note 143; Sabin Russell, *U.S. Push for Cheap Cipro Haunts AIDS Drug Dispute*, S.F. CHRON., Nov. 8, 2001, at A13, <https://www.sfgate.com/health/article/U-S-push-for-cheap-cipro-haunts-aids-drug-dispute-2860689.php>; see also Lauren Keller, *Ciprofloxacin and Compulsory Licensing of Pharmaceutical Patents* 12–13 (Apr. 23, 2002) (unpublished third-year paper), <https://dash.harvard.edu/handle/1/8852122>.

<sup>149</sup> See Sandra Sobieraj, *White House Mail Machine Has Anthrax*, WASH. POST (Oct. 23, 2011), [https://www.washingtonpost.com/wp-srv/aponline/20011023/aponline201158\\_000.htm](https://www.washingtonpost.com/wp-srv/aponline/20011023/aponline201158_000.htm).

<sup>150</sup> See Vanessa Fuhrmans, *Bayer May Ask Its Rivals for Help Producing Anthrax Antibiotic Cipro*, WALL ST. J. (Oct. 18, 2001), <https://www.wsj.com/articles/SB100334769597877200>; Robert Pear, *Government Talks with Drug Companies About Buying Antibiotics That Treat Anthrax*, N.Y. TIMES, Oct. 20, 2001, at B8.

into a concession of selling Cipro to the government at a fire-sale 50% discount.<sup>151</sup> Though HHS denied doing so in its public comments, Bayer's subsequent investor statements suggest that HHS did leverage its § 1498 powers to induce the deal.<sup>152</sup>

Throughout and after this patent squabble, Bayer and its supporters contended that the high patent-based prices for Cipro were necessary innovation incentives, not a profit-maximizing overcharge at the expense of the public.<sup>153</sup> Subsequent facts would point in a different direction. Two years later, in 2003, Bayer would plead guilty to Medicaid fraud and pay a \$257 million fine for a five-year-long scheme of overcharging the government for Cipro.<sup>154</sup>

### 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.<sup>155</sup>

Strong competition can thus complement national security by enhancing domestic cybersecurity, and patent assertion that unduly weakens competition

<sup>151</sup> See Keith Bradsher, *Bayer Agrees to Charge Government a Lower Price for Anthrax Medicine*, N.Y. TIMES, Oct. 25, 2001, at B8; *Bayer Agrees to Cut Cipro Price for Government After Administration Threatens to Override Patent*, KAISER HEALTH NEWS (June 11, 2009), <https://khn.org/morning-breakout/dr00007633/>.

<sup>152</sup> *Compare Nomination of Alex Michael Azar II: Hearing Before the S. Comm. on Finance*, 115th Cong. 119–20 (2018), <https://www.govinfo.gov/content/pkg/CHRG-115shrg34341/pdf/CHRG-115shrg34341.pdf> (“Bayer was never threatened with the use of section 1498”), with Bayer AG, Registration Statement (Form 20-F), at 10 (June 24, 2002), <https://www.sec.gov/Archives/edgar/data/1144145/000115697302000306/f00360e20vf.txt> (noting that U.S. government “contemplated compulsory licensing of our ciprofloxacin antibiotic”).

<sup>153</sup> See James Surowiecki, *No Profit, No Cure*, THE NEW YORKER (Oct. 29, 2001), <https://www.newyorker.com/magazine/2001/11/05/no-profit-no-cure>; Matthew Herper, *Cipro, Anthrax And The Perils Of Patents*, FORBES (Oct. 17, 2001), <https://www.forbes.com/2001/10/17/1017cipro.html>; Daniel R. Cahoy, *Treating the Legal Side Effects of Cipro: A Reevaluation of Compensation Rules for Government Takings of Patent Rights*, 40 AM. BUS. L.J. 125, 170–71 (2002); David B. Resnik & Kenneth A. De Ville, *Bioterrorism and Patent Rights: “Compulsory Licensure” and the Case of Cipro*, 2 AM. J. BIOETHICS 29, 37 (Summer 2002) (describing “the much coveted windfall drug breakthrough” as necessary “incentive to conduct financially lucrative and risky yet socially beneficial research”); Kayhan P. Parsi & Erin A. Egan, *Patents: The Public Interest Versus the Private Privilege*, 2 AM. J. BIOETHICS 45, 45 (Summer 2002) (“In fact, this strong financial incentive is what drives drug makers to spend millions of dollars in research and development . . .”).

<sup>154</sup> See Melody Petersen, *Bayer Agrees to Pay U.S. \$257 Million in Drug Fraud*, N.Y. TIMES, Apr. 17, 2003, at C1.

<sup>155</sup> See, e.g., DONALD J. TRUMP, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA 6 (Sept. 2018), <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf> (“Protecting American information networks, whether government or private, is vital to fulfilling” the objectives of “the National Security Strategy.”).

detracts from cybersecurity.<sup>156</sup> 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.<sup>157</sup> 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.<sup>158</sup> 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.<sup>159</sup> 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.<sup>160</sup> 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

---

<sup>156</sup> This is not to say that competition is the sole ingredient to increasing cybersecurity. As Paul Rosenzweig explains, there are appropriate regulatory measures to be taken to promote cybersecurity as well. See *Choosing the Right Cybersecurity Standards: Hearing Before the Subcomm. on Financial Institutions and Consumer Credit of the H. Comm. on Financial Services*, 115th Cong. (Feb. 14, 2018), available at <https://www.rstreet.org/2018/02/14/congressional-testimony-paul-rosenzweig-on-choosing-the-right-cybersecurity-standards/> (statement of Paul Rosenzweig).

<sup>157</sup> Chertoff, *supra* note 86.

<sup>158</sup> See Sadegh Farhang et al., *An Economic Study of the Effect of Android Platform Fragmentation on Security Updates*, 22 INT'L CONF. ON FIN. CRYPTOGRAPHY & DATA SECURITY 119, 127 (2018) (theorizing that in competitive software markets, “when consumers take into account security, then vendors have to invest to improve their security quality”).

<sup>159</sup> See Ashish Arora et al., *Competition and Patching of Security Vulnerabilities: An Empirical Analysis*, 22 INFO. ECON. & POL'Y 164, 165 (2010).

<sup>160</sup> See *id.* at 175.

as the degree of competitiveness in an industry increases.”<sup>161</sup> 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.<sup>162</sup> 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.”<sup>163</sup> 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.<sup>164</sup> 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.<sup>165</sup> Where a computer system such as Windows has a commanding share of users, a virus that exploits a flaw in that system can

<sup>161</sup> Esther Gal-Or & Anindya Ghose, *The Economic Incentives for Sharing Security Information*, 16 INFO. SYSTEMS RES. 186, 188 (2005).

<sup>162</sup> See Byung Cho Kim et al., *An Economic Analysis of the Software Market with a Risk-Sharing Mechanism*, 14 INT’L J. ELECTRONIC COM. 7, 9 (2009).

<sup>163</sup> Arrah-Marie Jo, *The Effect of Competition Intensity on Software Security—An Empirical Analysis of Security Patch Release on the Web Browser Market 3* (Dec. 2017) (unpublished manuscript), <https://www.tse-fr.eu/sites/default/files/TSE/documents/conf/ConfDigitalEconomy2018/Papiers/jo.pdf>.

<sup>164</sup> See, e.g., Lucian Armasu, *Qualcomm Firmware Vulnerabilities Expose 900 Million Devices, Including Security-Focused Smartphones*, TOM’S HARDWARE (Aug. 9, 2016), <https://www.tomshardware.com/news/quadroter-qualcomm-android-firmware-vulnerabilities,32414.html>; Ralf-Philipp Weinmann, *Baseband Attacks: Remote Exploitation of Memory Corruptions in Cellular Protocol Stacks 2*, in 6 PROC. USENIX WORKSHOP ON OFFENSIVE TECHS. (2012), <https://www.usenix.org/system/files/conference/woot12/woot12-final24.pdf>.

<sup>165</sup> See, e.g., Daniel E. Geer Jr., *Monoculture: Monopoly Considered Harmful*, IEEE SECURITY & PRIVACY, Nov.–Dec. 2003, at 14-17.

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.<sup>166</sup> 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.”<sup>167</sup>

There has been considerable study of the theory that computer monocultures are naturally more vulnerable to attacks.<sup>168</sup> 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.<sup>169</sup> 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.<sup>170</sup> By contrast, different versions of a single software product were found to share vulnerabilities 84.7% of the time.<sup>171</sup> 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.<sup>172</sup> 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.<sup>173</sup> The presence of systems from multiple vendors would mitigate these possibilities.

---

<sup>166</sup> See *id.*

<sup>167</sup> Yongguang Zhang et al., *Heterogeneous Networking: A New Survivability Paradigm*, NEW SECURITY PARADIGMS WORKSHOP 2001, at 33, 34 (Sept. 2001), <https://dl.acm.org/doi/pdf/10.1145/508171.508177>.

<sup>168</sup> See generally Benoit Baudry & Martin Monperrus, *The Multiple Facets of Software Diversity: Recent Developments in Year 2000 and Beyond*, ACM COMPUTING SURVS. art. 16, § 5.2 (Sept. 2015), <https://dl.acm.org/doi/pdf/10.1145/2807593>.

<sup>169</sup> See Jin Han et al., *On the Effectiveness of Software Diversity: A Systematic Study on Real-World Vulnerabilities*, 6 PROC. INT'L CONF. ON DETECTION OF INTRUSIONS & MALWARE, & VULNERABILITY ASSESSMENT 127, 129–30 (2009).

<sup>170</sup> See *id.* at 133–34.

<sup>171</sup> See *id.* at 140.

<sup>172</sup> See David Moore et al., *Inside the Slammer Worm*, IEEE SECURITY & PRIVACY, July–Aug. 2003, at 33, 37.

<sup>173</sup> Cf. Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program*, WALL ST. J. (Nov. 13, 2014), <https://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533> (discussing technology for surveillance of cell phone calls enabled by

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

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

---

a flaw in baseband processor security); Heath Hardman, *The Brave New World of Cell-Site Simulators*, 8 ALB. GOV'T L. REV. 1, 3 (2015).

<sup>174</sup> See, e.g., Randal C. Picker, *Cybersecurity: Of Heterogeneity and Autarky*, in *THE LAW AND ECONOMICS OF CYBERSECURITY* 115, 125 (Mark F. Grady & Francesco Parisi eds., 2005).

Picker proposes “autarky,” namely self-sufficiency of computers so that they can be disconnected from networks, as an alternative solution to monoculture. That proposal obviously is unworkable for connected devices.

<sup>175</sup> See Fred B. Schneider & Kenneth P. Birman, *The Monoculture Risk Put into Context*, IEEE SECURITY & PRIVACY, Jan.–Feb. 2009, at 14, 15.

<sup>176</sup> See *id.* at 16 (discussing “interface attacks”).

<sup>177</sup> See, e.g., Charles Duan, *Internet of Infringing Things: The Effect of Computer Interface Copyrights on Technology Standards*, 45 RUTGERS COMPUTER & TECH. L.J. 1, 11–12 (2019).

<sup>178</sup> See Chaim Gartenberg, *The 5G Standard Is Finally Finished with New Standalone Specification*, THE VERGE (June 15, 2018), <https://www.theverge.com/2018/6/15/17467734/5g-standalone-3gpp-standalone-finished>.

<sup>179</sup> See Lily Hay Newman, *5G Is More Secure than 4G and 3G—Except When It's Not*, WIRED (Dec. 15, 2019), <https://www.wired.com/story/5g-more-secure-4g-except-when-not/> (“Over the last year, [research scientist Ravishankar] Borgaonkar and other researchers have found and reported a number of security weaknesses in 5G . . .”).

<sup>180</sup> Cf. United States 5G Leadership Act of 2019, S. 1625, 116th Cong. § 9(a) (May 22, 2019).

competitive communication technology market is essential to cybersecurity and national security.

#### IV. LESSONS AND POLICY DIRECTIONS

The above discussion shows that patent protection can have mixed effects on national security: On the one hand, patents can encourage innovation that ensures domestic technological leadership and produces useful security-protective technologies; on the other hand, patents can stifle innovation-producing and cybersecurity-enhancing competition and can stymie the government's own ability to achieve national security goals. To navigate the complex effects of patent policy on national security, policymakers may consider the following recommendations as guideposts.

##### A. *Anticompetitive Patent Licensing*

An area of particular concern should be the use of patents and patent licensing strategies to diminish competition or put up roadblocks to new entrants. Policymakers should certainly not support these abuses of the patent system, and indeed should take steps to prevent them.

In the mobile communications space, patent licensing already plays an outsized role. There are reportedly between 250,000<sup>181</sup> and 314,000<sup>182</sup> patents on the smartphone alone, and litigation over cell phone technologies has lasted decades by now. Patents will thus inevitably have an impact on technologies like 5G or the Internet of Things, so the question is what that impact will be.

Patents are supposed to encourage innovation, but research finds that patents alone will not do so; competition is another requirement. A 2015 study considered the impact of competition policy and patent strength on innovation among European firms, measured in terms of research and development spending.<sup>183</sup> Initially, the study compared firms in countries with strong patent laws against those in countries with weaker patent laws, and found that patent protection has “no effect on R&D intensity,” a conclusion consistent with multiple other studies.<sup>184</sup> However, the study found that when a major

---

<sup>181</sup> See RPX Corp., Registration Statement (Form S-1), at 59 (Sept. 2, 2011), <https://www.sec.gov/Archives/edgar/data/1509432/000119312511240287/ds1.htm>.

<sup>182</sup> See Joel Reidenberg et al., *Patents and Small Participants in the Smartphone Industry*, 18 STAN. TECH. L. REV. 375, 382 tbl.2 (2015).

<sup>183</sup> See Philippe Aghion et al., *Patent Rights, Product Market Reforms, and Innovation*, 20 J. ECON. GROWTH 223, 230 (2015).

<sup>184</sup> *Id.* at 238; see Mariko Sakakibara & Lee Branstetter, *Do Stronger Patents Induce More Innovation? Evidence from the 1988 Japanese Patent Law Reforms*, 32 RAND J. ECON. 77, 78 (2001) (“We find no evidence of a statistically or economically significant increase in either R&D spending or innovative output that could plausibly be attributed to these reforms [to expand patent rights].”); Yi Qian, *Do National Patent Laws Stimulate Domestic Innovation in a Global Patenting Environment? A Cross-Country Analysis of Pharmaceutical Patent Protection, 1978–2002*, 89 REV. ECON. & STAT. 436, 450 (2007) (“I find no statistically significant relationship between national pharmaceutical patent protection and . . . domestic R&D.”).



competition reform went into effect, strong-patent countries enjoyed a boost in innovation greater than that experienced in weak-patent countries.<sup>185</sup> In other words, strong patent protection is complementary to strong competition; the former does not promote innovation without the latter. The practical import of this research is that patent protection is beneficial up to a point, but to the extent that patents—or, more commonly, legal strategies involving patents—overreach to suppress competition, that overreach should be cause for concern.

Yet today, strategic patent behavior contrary to competition is prevalent. The Federal Trade Commission's ongoing lawsuit against mobile phone chip manufacturer Qualcomm, for example, challenges Qualcomm's practice of refusing to sell chips to any phone manufacturer who does not first pay a hefty sum for patent licenses—even if the manufacturer does not actually have need for all those licenses.<sup>186</sup> To the extent that Qualcomm's "no license, no chips" practice is in fact anticompetitive—that is what the courts overseeing the case will decide—monopolization of that market could substantially harm cybersecurity for the reasons noted above.<sup>187</sup> The company's about-50% market share in the advanced mobile chip market<sup>188</sup> means that there is a virtual monoculture of Qualcomm chips already, and there are ongoing concerns about security vulnerabilities in those chips.<sup>189</sup> It is thus puzzling that some have opposed the FTC litigation on the grounds that it is making the United States "less competitive in the global 5G arms race."<sup>190</sup> As one scholar explains, this rhetoric "smacks of 'national champion' thinking" and ultimately fails to ensure that "national security warnings are being balanced against competitive imperatives."<sup>191</sup>

With respect to emerging information technologies, policymakers should be concerned that a leading firm could undertake similar patent licensing strategies to control the market. Indeed, the district court in the Qualcomm litigation found that Nokia and Ericsson already "have imitated Qualcomm's practice" because it is "more lucrative."<sup>192</sup>

---

<sup>185</sup> Aghion et al., *supra* note 183, at 243. Interestingly, the study finds this complementarity effect across patent-intensive industries—except for the computer and telecommunications industries. *Id.*

<sup>186</sup> See *supra* Part I.C.3.

<sup>187</sup> See *supra* Part III. It is, of course, possible that Qualcomm's practices are deemed not anticompetitive; in that case, the company need do no more than wait for the courts to vindicate that position.

<sup>188</sup> See Strategy Analytics 2018, *supra* note 53; Strategy Analytics 2019, *supra* note 53.

<sup>189</sup> See Weinmann, *supra* note 164, at 2; see also Armasu, *supra* note 164.

<sup>190</sup> Editorial Bd., *Peace in the Tech Patent Wars*, WALL ST. J. (Apr. 17, 2019), <https://www.wsj.com/articles/peace-in-the-tech-patent-wars-11555542274>.

<sup>191</sup> Claude Barfield, *In the 5G Race, Competition Policy Now Vies with Industrial and Security Policy*, AM. ENTERPRISE INST. (Apr. 22, 2019), <http://www.aei.org/publication/in-the-5g-race-competition-policy-now-vies-with-industrial-and-security-policy/>.

<sup>192</sup> Fed. Trade Comm'n v. Qualcomm Inc., 411 F. Supp. 3d 658, 755 (N.D. Cal. May 21, 2019), *appeal filed*, No. 19-16122 (9th Cir. argued Feb. 13, 2020).

If patents end up being used systematically to suppress competition in undue ways, then policymakers will need to pay greater attention to the consequences of those uses of patents for national security, and likely take legislative steps to reduce anticompetitive uses of patents. History provides a guide for doing so. The legislative response to American inferiority in pre-World War I aviation was the creation of a federal patent pool backed by federal permission to condemn patents on aircraft,<sup>193</sup> and the response to Bayer's hardball licensing of Cipro was for the government to use hardball negotiations backed by § 1498.<sup>194</sup>

### *B. Prizes, Grants, and Other Incentives for Innovation*

Patents are not the only incentive for innovation: Government policy may also encourage innovation through a variety of means, including prizes for inventions, research grants, and tax subsidies.<sup>195</sup> Each has its advantages and drawbacks: Patents offer theoretically market-based rewards but create perverse incentives due to monopoly rights; prizes and grants avoid anticompetitive opportunities but present moral hazard and valuation difficulties.<sup>196</sup>

Despite the many tradeoffs among different forms of innovation incentives, much of the literature and most policymakers have tended to gravitate toward patents as the default tool of innovation policy.<sup>197</sup>

The national security dimension of innovation in view of technological races, however, may suggest a need to alter that calculus. As seen above, patents can force a nation into dependence on a single supplier of critical technology, whether it be torpedoes, airplanes, or anthrax treatments.<sup>198</sup> Prizes or grants that allow for immediate free-market competition on any resulting inventions may have the benefit of protecting the government and the public from that single-supplier dependence. As a result, policymakers may seek to

<sup>193</sup> See Naval Service Appropriations Act, ch. 180, 39 STAT. 1168, 1169 (1917) (appropriating \$1,000,000 to the Secretary of War and Secretary of the Navy "to secure by purchase, condemnation, donation, or otherwise, such basic patent or patents as they may consider necessary to the manufacture and development of aircraft in the United States and its dependencies, for governmental and civil purposes"); Johnson, *supra* note 123, at 57.

<sup>194</sup> See *supra* Part II.C.

<sup>195</sup> See Daniel J. Hemel & Lisa Larrimore Ouellette, *Innovation Policy Pluralism*, 128 YALE L.J. 544, 551–52 (2019); Joseph E. Stiglitz, *Economic Foundations of Intellectual Property Rights*, 57 DUKE L.J. 1693, 1721 (2008).

<sup>196</sup> See Hemel & Ouellette, *supra* note 195, at 557 ("[N]o single innovation-incentive mechanism is uniformly superior in all circumstances."); Stiglitz, *supra* note 195, at 1722 tbl.1.

<sup>197</sup> See, e.g., Dan L. Burk & Mark A. Lemley, *Policy Levers in Patent Law*, 89 VA. L. REV. 1575, 1576 (2003) ("Patent law is our primary policy tool to promote innovation . . ."); Henry G. Grabowski et al., *The Roles of Patents and Research and Development Incentives in Biopharmaceutical Innovation*, 34 HEALTH AFF. 302, 302 (2015) ("[P]atents and regulatory exclusivity provisions are likely to remain the core approach to providing incentives for biopharmaceutical research and development.").

<sup>198</sup> See *supra* Part II.

divert innovators in security-sensitive technology fields away from patents by offering alternative rewards.

One difficulty is that because patent law generally applies uniformly to all types of technologies,<sup>199</sup> it may be difficult to leverage patent law itself to discourage patenting of those technologies that are of particular relevance to national security. Nevertheless, the government may leverage a variety of approaches, such as open licensing requirements in grant agreements or prize awards, or creation of patent pools with predefined licensing commitments, to limit the likelihood that exclusive rights arise in technology areas of concern to national security.

### C. *Economic Protectionism Versus Enhanced Competition*

The various recent instances of patents and national security discussed above have all carried at least some flavor of American competition against foreign nations, especially China. That places the patent–national security conversation well within the larger context of the Trump Administration’s general positions on economic nationalism and purported national security justifications for blocking foreign competitors.<sup>200</sup> The Trump Administration has taken numerous actions to limit the entry of foreign investment and competition, often justifying those actions on national security grounds; examples include the blocking of the Broadcom–Qualcomm merger by the Committee on Foreign Investment in the United States (CFIUS),<sup>201</sup> the various proposed and implemented bans on use of technology products made by

---

<sup>199</sup> See Brad A. Greenberg, *Rethinking Technology Neutrality*, 100 MINN. L. REV. 1495, 1560–61 (2016). But see Dan L. Burk & Mark A. Lemley, *Is Patent Law Technology-Specific?*, 17 BERKELEY TECH. L.J. 1157, 1205 (2002) (arguing that “[p]atent law is becoming technology-specific”).

<sup>200</sup> See, e.g., Inaugural Address, DAILY COMP. PRES. DOC. No. 58, at 2 (Jan. 20, 2017), <https://www.govinfo.gov/content/pkg/DCPD-201700058/pdf/DCPD-201700058.pdf> (“We must protect our borders from the ravages of other countries making our products, stealing our companies, and destroying our jobs.”); Douglas A. Irwin, *The False Promise of Protectionism: Why Trump’s Trade Policy Could Backfire*, FOREIGN AFF., May–June 2017, at 45, 45.

<sup>201</sup> See *supra* Part I.C.1.

Chinese firms such as Huawei and ZTE,<sup>202</sup> and the steel and aluminum tariffs.<sup>203</sup>

As a general matter, there are questions of whether these border-closing measures are genuine protections from security threats or thinly veiled economic protectionism.<sup>204</sup> Even putting those questions aside, though, one ought to be skeptical of the relevance of economic nationalism to patent policy for a simple reason: The benefits of patents do not accrue solely to American firms. The United States, as a signatory to the TRIPS Agreement, is obligated to make patent protection available to foreigners on equal terms.<sup>205</sup> As the Verizon–Huawei patent dispute shows, foreign firms can use U.S. patents to interfere with domestic businesses.<sup>206</sup> That seemingly reversed situation of foreign patent holders asserting American patents against American companies is likely to recur, especially given that foreign inventors receive a large share of currently issued patents: Chinese inventors received 11,241 U.S. patents in 2017, making it one of the top five patent recipient nations that year.<sup>207</sup> If policymakers hope to protect national security through innovation policy, then, they ought to consider that patent protection can have the counterintuitive effect of enabling foreign companies to stymie American efforts.

#### D. *Protecting the Government Itself: The 2018 NDAA*

Besides protecting competition and the public at large from harmfully aggressive uses of patents, policymakers ought also to be concerned with protecting the government itself from aggressive patent licensing. One commonality among the three historical examples given earlier<sup>208</sup> is that when

---

<sup>202</sup> See, e.g., Eric Geller, *Trump Likely to Sign Executive Order Banning Chinese Telecom Equipment Next Week*, POLITICO (Feb. 7, 2019), <https://www.politico.com/story/2019/02/07/trump-ban-chinese-telecom-1157090> (proposed ban on Huawei phones); Jacob Kastrenakes, *Trump Signs Bill Banning Government Use of Huawei and ZTE Tech*, THE VERGE (Aug. 13, 2018), <https://www.theverge.com/2018/8/13/17686310/huawei-zte-us-government-contractor-ban-trump>; Damian Paletta et al., *Trump Administration Cracks Down on Giant Chinese Tech Firm, Escalating Clash with Beijing*, WASH. POST (May 15, 2019), [https://www.washingtonpost.com/world/national-security/trump-signs-order-to-protect-us-networks-from-foreign-espionage-a-move-that-appears-to-target-china/2019/05/15/d982ec50-7727-11e9-bd25-c989555e7766\\_story.html](https://www.washingtonpost.com/world/national-security/trump-signs-order-to-protect-us-networks-from-foreign-espionage-a-move-that-appears-to-target-china/2019/05/15/d982ec50-7727-11e9-bd25-c989555e7766_story.html) (placement of Huawei on the entity list, which “forces Huawei and its affiliates to obtain a U.S. government license to buy American technology”); Cecilia Kang & David E. Sanger, *Huawei Is a Target as Trump Moves to Ban Foreign Telecom Gear*, N.Y. TIMES (May 15, 2019), <https://www.nytimes.com/2019/05/15/business/huawei-ban-trump.html>.

<sup>203</sup> See sources cited *supra* notes 29–30.

<sup>204</sup> See *id.*; Irwin, *supra* note 200, at 45 (arguing that President Trump’s “brand of economic nationalism is just one step away from old-fashioned protectionism”).

<sup>205</sup> See TRIPS Agreement, *supra* note 105, art. 3, ¶ 1.

<sup>206</sup> See *supra* Part I.D.

<sup>207</sup> See Susan Decker, *China Becomes One of the Top 5 U.S. Patent Recipients for the First Time*, BLOOMBERG (Jan. 9, 2018), <https://www.bloomberg.com/news/articles/2018-01-09/china-enters-top-5-of-u-s-patent-recipients-for-the-first-time>.

<sup>208</sup> See *supra* Part II.

the government itself is the buyer of patented technologies, it can easily become the victim of costly licensing schemes.

Indeed, Congress has recently recognized this need to protect the government in intellectual property licensing negotiations generally. Section 802 of the National Defense Authorization Act for Fiscal Year 2018 requires the Secretary of Defense to develop policy to ensure that government license negotiators “are aware of the rights afforded the Federal Government and contractors in intellectual property” and that they “fully consider and use all available techniques and best practices for acquiring or licensing intellectual property.”<sup>209</sup> It further creates a “cadre” of IP experts to assist military departments on “financial analysis and valuation of intellectual property” and “communications and negotiations with contractors.”<sup>210</sup>

Legislative history confirms that section 802 is intended to protect the government during licensing negotiations. The House report observes within the Department of Defense “varying knowledge of IP matters” and expresses concern that “inconsistency and lack of coordination disadvantages the Department” such that “the Department requires tools to improve its ability to negotiate with industry.”<sup>211</sup> The conference report similarly characterizes the IP cadre as supporting Department staff to “develop their IP strategies and negotiate with industry.”<sup>212</sup>

Subsequent developments are of the same effect. In a press briefing, Undersecretary of Defense Ellen M. Lord explained that the purpose of the IP cadre was to avoid “problems with intellectual property when we don’t clearly define what is owned by industry, and what will be owned by government.”<sup>213</sup> Law firms specializing in government contracts describe section 802 as “designed to ensure that DoD does not leave rights on the table when it negotiates the scope of IP rights,”<sup>214</sup> and even advise contractors to “beware” that section 802 “will make the DoD a more effective purchaser of IP.”<sup>215</sup>

---

<sup>209</sup> National Defense Authorization Act for Fiscal Year 2018 § 802(a)(2), 10 U.S.C. § 2322 (2018).

<sup>210</sup> *Id.* §§ 802(b)(3)(C), (E).

<sup>211</sup> H.R. REP. NO. 115-200, pt. 1, at 165 (2017), <https://www.congress.gov/115/crpt/hrpt200/CRPT-115hrpt200.pdf>.

<sup>212</sup> H.R. CONF. REP. NO. 115-404, at 863 (2018), <https://www.congress.gov/115/crpt/hrpt404/CRPT-115hrpt404.pdf>.

<sup>213</sup> Ellen M. Lord, Press Briefing on Acquisition Reform and Innovation (Aug. 26, 2019), <https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/1944326/undersecretary-of-defense-lord-holds-press-briefing-on-acquisition-reform-and-i/>. Undersecretary Lord’s response is notable because she limits the IP cadre to this domestic defensive task, rejecting the idea that the cadre has an “offensive” role in dealing with Chinese IP theft or such issues. *See id.* (question by Aaron Mehta, Defense News).

<sup>214</sup> Mary Beth Bosco, *2018 NDAA Analysis: Intellectual Property Provisions*, HOLLAND & KNIGHT GOV’T CONT. BLOG (Dec. 12, 2017), <https://www.hklaw.com/en/insights/publications/2017/12/2018-ndaa-analysis-intellectual-property-provision>.

<sup>215</sup> Adam Bartolanzo & Keith Szeliga, *Contractors Beware: The 2018 NDAA Ushers In New Changes Affecting IP Rights*, GOV’T CONT. & INVESTIGATIONS BLOG (Jan. 30, 2018), <https://www.governmentcontractslawblog.com/2018/01/articles/department-of-defense/ndaa-ip-rights/>.

The 2018 NDAA demonstrates an ongoing concern that IP licensing can interfere with American national defense operations, and that policy solutions are necessary to resist aggressive licensing. It is perhaps unfortunate, then, that the Department of Defense concedes its vulnerability to a contractor's patent licensing practices and indeed says that the government's operations depend on that contractor's patent licensing remaining untouched, at the same time that Congress has instructed the Department of Defense to negotiate forcefully against its contractors' patent licensing practices.<sup>216</sup> Both Congress and federal agencies such as the Department of Defense should continue to be aware of how intellectual property licensing practices can set back the government and thus set back national security, and push back rather than acquiesce in those licensing practices.

### CONCLUSION

This article has looked at the recent policy conversations on patents and national security, and questioned a common line of reasoning in those conversations, namely an argument that increased patent protection will increase national security. Both historical evidence and modern research into cybersecurity offer reasons to dispute that argument. With regard to history, patents have on multiple notable occasions interfered with the U.S. government's ability to prepare for war or protect the public from terrorism, leaving the government forced to take sometimes forceful measures to resist assertions of patent rights in the name of national security. With regard to cybersecurity, economic and computer science research suggests that robust competition enhances cybersecurity by giving technology firms market-based incentives to secure their products, and by preventing vulnerable monocultures from arising. Insofar as patents can suppress competition, patents can thus be in tension with cybersecurity and national security. Based on these identified tensions and historical predicaments, the article recommends that policymakers take steps to account for the nuanced relationship between patents and national security, and in particular focus on policies that enhance competition rather than imposing patents on technologies necessary to protecting the public.

---

<sup>216</sup> See DOD Declaration, *supra* note 82, ¶¶ 6-7.

