Submitted Statement for the Record of

Charles Duan
Director, Technology & Innovation Policy
R Street Institute

Before the

Committee on the Judiciary
United States Senate

Hearing on

5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation

May 14, 2019

5G: NATIONAL SECURITY CONCERNS, INTELLECTUAL PROPERTY ISSUES, AND THE IMPACT ON COMPETITION AND INNOVATION
SUBMITTED STATEMENT OF CHARLES DUAN

Chairman Graham, Ranking Member Feinstein, and Members of the Committee:

Thank you for holding this hearing on 5G, national security, intellectual property, and the impact on competition and innovation. As wireless communication technologies become more pervasive and ubiquitous, cybersecurity in communications takes on a greater role in protecting both individual consumers and national security as a whole. New technological phenomena such as 5G networks and the Internet of Things hold great promise but also great risk.

My name is Charles Duan, and I am the Director for Technology and Innovation Policy at the R Street Institute, a nonprofit, nonpartisan public policy research organization. Our mission is to engage in policy research and outreach to promote free markets and limited, effective government in many areas, including competition and growth in the technology sector. This statement represents my individual views and does not necessarily reflect the views of other scholars at the R Street Institute.

As the Committee contemplates ways of ensuring cybsersecurity, it should focus especially on the classic American strategy for success in all commercial endeavors: competition in the market. Strong competition among private firms has long been a recipe for innovation, growth, and consumer welfare. Competition also increases cybersecurity. As explained below, extensive economic research finds that competition encourages technology firms to patch security vulnerabilities, invest in stronger cybersecurity, and protect their customers to a greater degree. Furthermore, competition prevents a troubling phenomenon known in computer science circles as a "monoculture," in which a technological ecosystem dominated by a single product or vendor catastrophically fails, potentially taking down critical infrastructure. Diversity in products and services, fostered by competition among a diversity of firms in the market, can help to avoid these cybersecurity threats.

There are at least three ways to promote competition in emerging technology markets such as 5G and the Internet of Things (or "IoT"). First, this Committee should seek to reduce barriers that prevent new firms from entering markets, and avoid efforts to stymie new entrants. This is acutely important in view of numerous calls to block foreign companies in the name of national security; the national security concerns are not to be ignored, but they must be evaluated and weighed against their competition-limiting effects. Second, the Committee should look to curtail anticompetitive practices within industries. The ongoing use of complex patent licensing strategies within the telecommunications sector is especially concerning from a competition standpoint, and it warrants serious investigation. Third, the Committee should consider the ways in which regulatory barriers to the use of new technologies can have disproportionate impact on small firms and thus unintentionally entrench incumbents, potentially to the detriment of cybersecurity.

I. Competition Ensures Cybersecurity in Emerging Communication Technologies

To ensure cybersecurity in a world of ubiquitous devices, an essential component is competition among firms up and down the vertical chain.[1] 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.

[1]This is not to say that competition is the sole ingredient to increasing cybersecurity. As my colleague Paul Rosenzweig explains, there are appropriate regulatory measures to be taken to promote cybersecurity as well. Testimony of Paul Rosenzweig, Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Financial Services, "Choosing the Right Cybersecurity Standards," 115th Congress (GPO, Feb. 14, 2018), https://www.rstreet.org/2018/02/14/congressional-testimony-paul-rosenzweig-on-choosing-the-right-cybersecurity-standards/.

A. Economic Research Demonstrates That Competition Drives Firms to Produce More Secure Products

Economic research shows that monopolists are unlikely to follow good cybersecurity practices. Thus, avoidance of market concentration increases the likelihood that firms will produce more secure products. Intuitively, this makes sense: Computer security is a value-added benefit to consumers, so firms in competitive markets are likely to use security improvements to gain an edge over their competitors, and are likely to poke holes in their competitors' products to draw consumers away from them. By contrast, monopolized markets offer less external impetus to test products for flaws, and a monopolist may choose to focus less on security and more on new product features or increased product quality.

Economic research confirms these hypoetheses 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.[2] 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.[3] Similarly, in 2005 business researchers modeled incentives for firms to share cybersecurity information, and concluded that the "inclination to share information and invest in security technologies increases as the degree of competitiveness in an industry increases."[4] Another study concluded 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

---

[2]Ashish Arora, Chirs Forman, Anand Nandkumar and Rahul Telang, "Competition and Patching of Security Vulnerabilities: An Empirical Analysis," *Information Economics and Policy* 22 (2010), p. 165, https://www.heinz.cmu.edu/~rtelang/IEP_patching.pdf.

[3]Ibid., p. 175.

[4]Esther Gal-Or and Anindya Ghose, "The Economic Incentives for Sharing Security Information," *Information Systems Research* 16 (2005), p. 188, https://pubsonline.informs.org/doi/10.1287/isre.1050.0053.

responsibility.[5] To be sure, an unpublished study from 2017 finds that greater 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."[6] This research confirms that competition is conducive to cybersecurity improvement.

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. The best way to get ahead of ongoing and future cybersecurity issues is to ensure the presence of adversarial competition in the market.

B. Competition Prevents the Creation of Monocultures That Are Especially Vulnerable to Cyberattacks

Monopoly also undermines cybersecurity because it can create a "monoculture" of single-vendor products, opening the door to massive systemic failure in the case of a cyberattack. Computer researchers developed the concept 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.[7] When a computer system such as Windows has a dominant share of users, a virus that exploits a flaw in that system can quickly spread to infect numerous systems. An operating system monopoly thus enabled the fast and easy spread

---

[5]Byung Cho Kim, Pei-yu Chen and Tridas Mukhopadhyay, "An Economic Analysis of the Software Market with a Risk-Sharing Mechanism," *International Journal of Electronic Commerce* 14:2 (2009), p. 9, https://www.tandfonline.com/doi/abs/10.2753/JEC1086-4415140201.

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

[7]See, e.g., Daniel E. Geer Jr., "Monoculture: Monopoly Considered Harmful," *IEEE Security and Privacy*, Nov.–Dec. 2003, https://ieeexplore.ieee.org/abstract/document/1253563.

of cyberattacks, and better cybersecurity could have been facilitated by greater diversity in online systems.[8] 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."[9]

There has been considerable study of the theory that computer monocultures are naturally more vulnerable to attacks. To support this theory, researchers have found that software substitutes generally do not share the same flaws: Of 2,627 software vulnerabilities reported in 2007, only 29 (1.1%) applied to two products providing the same functionality.[10] By contrast, different versions of a single software product were found to share vulnerabilities 84.7% of the time.[11] 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 or the Internet of Things, 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. A monoculture that is vulnerable to so-called "rootkits" or "backdoors"—maliciously installed software that enable bad actors to commandeer systems—could also

---

[8]Ibid.

[9]Yongguang Zhang, Harrick Vin, Lorenzo Alvisi, Wenke Lee and Son K. Dao, "Heterogeneous Networking: A New Survivability Paradigm," *Proceedings of the Workshop on New Security Paradigms* 2001 (2001), p. 34.

[10]Jin Han, Debin Gao and Robert H. Deng, "On the Effectiveness of Software Diversity: A Systematic Study on Real-World Vulnerabilities," *Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* 6 (2009), pp. 133–34.

[11]Ibid., p. 140.

enable mass surveillance or spying by private hackers or foreign governments.[12] The presence of systems from multiple vendors would mitigate these possibilities.

The monoculture theory is not without critics, but a review of those criticisms shows them to be inapplicable to contemporary communication technologies. Some critics suggest that software diversity imposes unwarranted costs on firms who must forego economies of scale and devise seemingly duplicative yet different setups of computer systems.[13] 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.[14] 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).[15]

It is widely recognized that a monoculture is unavoidable in at least one respect: Most connected devices will need to conform to technical standards. Internet of Things devices generally communicate over wireless protocols such as Wi-Fi or Bluetooth, and 5G

---

[12]Cf. Devlin Barrett, "Americans' Cellphones Targeted in Secret U.S. Spy Program," *Wall Street Journal*, Nov. 13, 2014 (discussing technology for surveillance of cell phone calls enabled by a flaw in baseband processor security), https://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533; Heath Hardman, "The Brave New World of Cell-Site Simulators," *Albany Government Law Review* 8 (2015), p. 1.

[13]See, e.g., Randal C. Picker, "Cybersecurity: Of Heterogeneity and Autarky", in *The Law and Economics of Cybersecurity* (Mark F. Grady and Francesco Parisi eds., 2005), pp. 115, 125. 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.

[14]Fred B. Schneider and Kenneth P. Birman, "The Monoculture Risk Put into Context," *IEEE Security and Privacy*, Jan.–Feb. 2009, p. 15.

[15]Ibid. (discussing "interface attacks").

itself is a technical standard developed by private industry. A flaw in any such standard would render all mobile devices implementing the standard vulnerable to an identical attack. The best defense against this especially catastrophic possibility is rigorous development and testing of standards. The best way to ensure rigorous development and testing is to ensure that as many firms as possible, especially firms that share basic American values, are involved in the development of those standards. Thus, the necessary standardization of information and communication technologies is perhaps the most important reason why a competitive communication technology market is essential to cybersecurity and national security.

II. Competition Also Spurs Innovation and Promotes Success Among Domestic Industries

Although competition is critical to ensuring cybersecurity, it also is necessary to stimulate innovation overall.

When firms are closely matched in their abilities to develop cutting-edge technologies (in the terminology of economists, both are "close to the technological frontier"), competition provides incentives for all of those firms to innovate such that they can leapfrog ahead and "escape" competition temporarily.[16] A 2009 empirical study confirmed that incumbent firms close to the technological frontier have strong incentives to innovate in the face of competition in order to "escape" that competition with better products.[17] Similarly, economists theorize that innovative growth in duopoly markets occurs in a "step-by-step" fashion requiring a degree of copying between competitors, such that "a little imitation is

[16]Philippe Aghion, Nick Bloom, Richard Blundell, Rachel Griffith and Peter Howitt, "Competition and Innovation: An Inverted-U Relationship," *Quarterly Journal of Economics* 120 (2005), p. 702, https://www.ucl.ac.uk/~uctp39a/ABBGH_QJE_2005.pdf.

[17]Philippe Aghion, Richard Blundell, Rachel Griffith, Peter Howitt and Susanne Prantl, "The Effects of Entry on Incumbent Innovation and Productivity," *Review of Economics and Statistics* 91 (2009), pp. 21–22, 27, https://dash.harvard.edu/bitstream/handle/1/4554222/aghion_incumbent.pdf.

almost always growth-enhancing" by "promoting more frequent neck-and-neck rivalry."[18] These studies all confirm that competition is important to stimulating innovation.

III. To Promote Cybersecurity, Congress Should Promote Competition and Oppose Efforts to Undermine It

Given that competition offers these benefits to cybersecurity and innovation, this Committee and Congress should focus on promoting competition and removing entry barriers in new technology markets, especially among domestic firms. This focus is especially important because incumbent firms have long advocated, and continue today to advocate, for policies that effectively ask the government to pick winners and losers, to create artificial barriers to entry for newcomer competitors, and to allow for monopolization that diminishes incentives toward product quality and security.

A. Promoting New Entrants Versus Excluding Foreign Companies

Much attention has been paid to blocking entry of foreign company products out of cybersecurity or national security concerns. This has been the basis for the blocking of the Broadcom–Qualcomm merger by the Committee on Foreign Investment in the United States (CFIUS),[19] the proposed federal ban on Huawei mobile phones,[20] the steel and aluminum tariffs,[21] and the recent move to prevent Huawei from purchasing American chips, software, and other technologies.[22]

---

[18]Philippe Aghion, Christopher Harris, Peter Howitt and John Vickers, "Competition, Imitation and Growth with Step-by-Step Innovation," *Review of Economic Studies* 68 (2001), p. 470, https://dash.harvard.edu/handle/1/12375013.

[19]Cecilia Kang and Alan Rappeport, "Trump Blocks Broadcom's Bid for Qualcomm," *The New York Times*, Mar. 12, 2018, https://www.nytimes.com/2018/03/12/technology/trump-broadcom-qualcomm-merger.html.

[20]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. No executive order appears to have been signed so far.

[21]Clark Packard and Megan Reiss, "Steel Protectionism Won't Protect National Security," *Lawfare*, Jan. 12, 2018, https://www.lawfareblog.com/steel-protectionism-wont-protect-national-security.

[22]Cecilia Kang and David E. Sanger, "Huawei Is a Target as Trump Moves to Ban Foreign Telecom Gear," *The New York Times*, May 15, 2019, https://www.nytimes.com/2019/05/15/business/huawei-ban-trump.html.

Where there are in fact genuine concerns for cybersecurity or national security—known vulnerabilities in devices, for example[23]—it is obviously appropriate for the government to take action to avoid harms to the nation. But it should be remembered that any sort of exclusionary activity against foreign competitors is a government intervention to suppress competition. Many have expressed concerns that allegations of national security harms are covers for economic protectionism,[24] the consequence of which is potentially less competition and thus, for the reasons discussed above, less cybersecurity.

Congress should thus approach invocations of cybersecurity threats with a dispassionate eye, considering the consequences for competition of imposing restraints on trade in the name of security. By the same token, to the extent that Congress considers measures to increase security, its first line of approach should be reducing entry barriers to new startup firms, in order to increase competition. As Caleb Watney at the R Street Institute explains, there are simple pathways to expanding opportunities in emerging technological fields, such as addressing shortages of skilled labor and making computing resources that already exist more readily available to startups.[25] These sorts of approaches would likely build up new firms that would maintain competitive pressure, leading to better cybersecurity.

B. Limiting Anticompetitive Patent Licensing Strategies

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. Congress should

---

[23]Huawei Cyber Security Evaluation Center Oversight Board, *Annual Report to the National Security Adviser of the United Kingdom* (Mar. 2019), para. 5.4, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

[24]Packard and Reiss, https://www.lawfareblog.com/steel-protectionism-wont-protect-national-security; Noah Feldman, "Huawei and 5G: A Case Study in the Future of Free Trade," *Bloomberg Opinion*, Feb. 13, 2019, https://www.bloomberg.com/opinion/articles/2019-02-13/huawei-and-5g-a-case-study-in-the-future-of-free-trade.

[25]Caleb Watney, "Reducing Entry Barriers in the Development and Application of AI," R Street Policy Study No. 153, Oct. 2018, https://www.rstreet.org/2018/10/09/reducing-entry-barriers-in-the-development-and-application-of-ai/.

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[26] and 314,000[27] 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.[28] Initially, the study compared firms in countries with strong patent laws against those in countries with weaker patent laws, and "found no effect of patent protection on R&D intensity," a conclusion consistent with multiple other studies.[29] However, the study found that when a major competition reform went into effect, strong-patent countries enjoyed a boost in innovation greater than that experienced in weak-patent countries.[30] In other words, strong patent protec-

---

[26]RPX Corporation, Registration Statement (Form S-1), at p. 59 (Sept. 2, 2011), https://www.sec.gov/Archives/edgar/data/1509432/000119312511240287/ds1.htm.

[27]Joel Reidenberg et al., "Patents and Small Participants in the Smartphone Industry," *Stanford Technology Law Review* 18 (2015), p. 382 tbl.2, https://ir.lawnet.fordham.edu/faculty_scholarship/640/.

[28]Philippe Aghion, Peter Howitt and Susanne Prantl, "Patent Rights, Product Market Reforms, and Innovation," *Journal of Economic Growth* 20 (2015), p. 230.

[29]Ibid., p. 238; Mariko Sakakibara and Lee Branstetter, "Do Stronger Patents Induce More Innovation? Evidence from the 1988 Japanese Patent Law Reforms," *RAND Journal of Economics* 32 (2001), p. 78 ("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," *Review of Economics and Statistics* 89 (2007), p. 450 ("I find no statistically significant relationship between national pharmaceutical patent protection and . . . domestic R&D.").

[30]Aghion, Howitt and Prantl, p. 243. Interestingly, the study finds this complementarity effect across patent-intensive industries—except for the computer and telecommunications industries. Ibid.

tion 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.

To the extent that Qualcomm's "no license, no chips" practice is in fact anticompetitive—that is what the district court overseeing the case will decide—monopolization of that market could substantially harm cybersecurity for the reasons noted above.[31] The company's over-50% market share in the advanced mobile chip market[32] means that there is a virtual monoculture of Qualcomm chips already, and there are ongoing concerns about security vulnerabilities in those chips.[33] It is thus puzzling that some have opposed the FTC litigation on the grounds that it is "making the US less competitive in the global 5G arms race." As one scholar explains, this rhetoric "smacks

---

[31]It is, of course, possible that Qualcomm's practices are not anticompetitive; in that case, the company need do no more than wait for the district court to vindicate that position.

[32]"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.

[33]Ralf-Philipp Weinmann, "Baseband Attacks: Remote Exploitation of Memory Corruptions in Cellular Protocol Stacks" p. 2, in 6 *Proceedings of the USENIX Workshop on Offensive Technologies* (2012), https://www.usenix.org/system/files/conference/woot12/woot12-final24.pdf; see also Lucian Armasu, "Qualcomm Firmware Vulnerabilities Expose 900 Million Devices, Including Security-Focused Smartphones," *Tom's Hardware*, Aug. 9, 2016, https://www.tomshardware.com/news/quadrooter-qualcomm-android-firmware-vulnerabilities,32414.html.

of 'national champion' thinking" and ultimately fails con ensure that "national security warnings are being balanced against competitive imperatives."[34]

With respect to emerging information technologies, Congress should be equally concerned that a leading firm could undertake similar patent licensing strategies to control the market. Network infrastructure, wireless protocols, and software are all areas where complex patent litigation has arguably created substantial barriers to entry. Patent practices ought to be scrutinized skeptically for the effects they may have on competition and thus security.

C. Avoiding Regulatory Measures That Disproportionately Burden Smaller Competitors

Regulatory efforts directed at technology firms could entrench incumbents, limit competition, and impede cybersecurity. At a very high level, regulation imposes costs of compliance on businesses. To the extent that large firms are better able to absorb those costs of compliance, either due to economies of scale or because the regulatory scheme imposes one-size-fits-all obligations on small and big firms alike, the potential consequence of the regulation could be to entrench large incumbents and stymie competition.

There are several areas in which Congress is considering engaging in regulatory legislation relating to communication technologies, and each of those areas warrants consideration as to effects on competition. Privacy legislation is one such topic that my colleagues have noted previously: Compliance with privacy protections can be easier for larger firms than for small ones, so the (certainly important) public value of greater privacy must be weighed against any potential hindrance to competition.[35] Directives re-

---

[34]Claude Barfield, "In the 5G Race, Competition Policy Now Vies with Industrial and Security Policy," *American Enterprise Institute*, Apr. 22, 2019, http://www.aei.org/publication/in-the-5g-race-competition-policy-now-vies-with-industrial-and-security-policy/.

[35]Letter from Tom Struble et al., R Street Institute, to Janice D. Schakowsky and Cathy McMorris Rodgers, Subcommittee on Consumer Protection and Commerce, House Energy and Commerce Committee, "Hearing on 'Protecting Consumer Privacy in the Era of Big Data' " (Feb. 26, 2019), https://www.rstreet.org/2019/02/26/letter-regarding-hearing-on-protecting-consumer-privacy-in-the-era-of-big-data/. This will also be the subject of forthcoming research from the R Street Institute.

lating to content moderation are another, since there are substantial economies of scale present in online platforms' ability to review posted user content.[36]

This is not to say that any regulatory efforts ought to be avoided per se, but they do need to be considered carefully to the extent that they could present barriers to new entrants or barriers to strong competition. And in particular with regard to cybersecurity, attention must be paid to whether regulatory schemes may interfere with private development of cybersecurity technologies and norms. Industry working groups have long been developing consensus views on cybersecurity practices for 5G and the Internet of Things.[37] Robust industry collaboration on cybersecurity depends on high levels of competition and thus low barriers to entry that foster competition.

IV. Conclusion

I thank the Committee for its attention to the matters presented above. If my colleagues at the R Street Institute or I can be of any assistance to members of the Committee, please feel free to contact me.

---

[36]Jeffrey Westling, "Deep Fakes: Let's Not Go Off the Deep End," *Techdirt*, Jan. 30, 2019, https://www.techdirt.com/articles/20190128/13215341478/deep-fakes-lets-not-go-off-deep-end.shtml.

[37]See, e.g., Communications Security, Reliability and Interoperability Council, *Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks* (v14.0 ed. Sept. 2018), https://www.fcc.gov/files/csric6wg3sept18report5gdocx-0.