June 17, 2019

VIA REGULATIONS.GOV

Ambassador Robert E. Lighthizer
U.S. Trade Representative
Office of the United States Trade Representative
600 17th Street NW
Washington, DC 20006


Dear Ambassador Lighthizer:

On behalf of Fitbit, Inc. (“Fitbit”), we hereby submit the following written comments regarding the United States Trade Representative’s (“USTR”) May 17, 2019 Proposed Modification of Action Pursuant to Section 301: China’s Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation.¹ Last year, the U.S. Trade Representative (“USTR”) announced its intention to impose additional tariffs under “List 3” on $200 billion in goods imported from China.² USTR’s proposal included goods entered under subheading 8517.62.00 of the Harmonized Tariff Schedule of the United States, a tariff line that covers wireless products, including the fitness trackers and smartwatches that comprise nearly all of Fitbit’s products. After receiving

---


comments and testimony from Fitbit, among others, USTR determined to remove such products from the finalized scope of the $200 billion tariff action. As discussed below, Fitbit believes that the same concerns that led USTR to remove these products from the scope of List 3 continue to apply.

Fitbit therefore respectfully requests that USTR remove HTSUS subheading 8517.62.0090 from the scope of the Proposed Modification of Action currently under consideration as well. Alternatively, USTR should remove wearable devices such as fitness trackers and smart watches classifiable under this subheading. At the very least, Fitbit urges USTR to delay implementation of the tariff with respect to these products to allow additional time for consideration of the issues discussed herein. A 25% tariff on these products would (i) cause significant and unavoidable economic harm to American companies like Fitbit and the U.S. economy, (ii) have the perverse effect of advancing primary Chinese objectives under Made in China 2025 and related industrial policy plans, and (iii) compromise U.S. national security and user privacy, without addressing the problems identified in USTR’s Section 301 Report.

background on fitbit

Fitbit is one of the world’s leading brands for wearable devices, primarily health and fitness trackers and smart watches, with more than 93 million devices sold. Our mission is to give our users the data, inspiration and guidance they need to improve their health, while transforming the healthcare system and reducing healthcare costs. Our devices are assembled in China using components sourced from suppliers worldwide. They are sold in more than
15,000 retail stores across the United States and in more than 45,000 retail stores in 86 countries around the world.

While Fitbit’s operations are global, it is very much an American company. Fitbit is headquartered in San Francisco, with facilities in Boston, MA; San Diego, CA; and Issaquah, WA, and its Americas logistics hub in Indiana. Fitbit employs more than 1,700 people, seventy-five percent of whom are based in the United States. In recent years, Fitbit’s U.S. operations have accounted for over 90% of our total operating expenditures. These operations encompass far more than fitness trackers and smart watches. Fitbit maintains one of the world’s largest databases of validated health data, including data relating to more than 9 billion nights of sleep, 181 billion hours of heart rate tracking, 142 trillion steps, and 250 billion minutes of exercise. This data, in turn, supports one of the world’s largest health and fitness social networks, comprising more than 27 million active users tracking their progress on one of the United States’ leading health and fitness app for iOS and Android devices.

Fitbit also partners with more than 1,500 companies in the United States, from small- and medium-sized business to Fortune 500 companies, in corporate wellness programs to promote and improve employee health. Fitbit’s corporate wellness partners have included BP, Bank of America, IBM, Kimberly-Clark, and Time Warner. Studies have shown that wellness programs like these can save as much as 25% per person in total healthcare costs. In a 2014 survey of

---


employees participating in corporate wellness programs with Fitbit products, 67% reported eating better, 63% reported leading more active lifestyles, 68% reported better weight management, and 67% reported coping more effectively with stress. Results like these have led more than 100 health plans across the country to offer Fitbit products as part of their efforts to improve Americans’ health and lower healthcare costs, and more than 800 clinical trials to use Fitbit products in pursuing improved health outcomes for all Americans.

Fitbit’s healthcare partnerships extend to the public sector as well. In January 2018, Fitbit was one of only nine companies selected from more than 100 applicants to participate in the Food and Drug Administration’s digital Health Software Precertification Program. This program aims to assist the agency’s “development of a regulatory model to assess the safety and effectiveness of software technologies without inhibiting patient access to these technologies.” Fitbit is thus playing an active role in efforts by both the U.S. government and U.S. businesses to use technology to lower healthcare costs while improving patient outcomes. Reflecting the breadth of its operations and goals as a company, Fitbit invested $313 million in R&D in 2018 alone, primarily in the United States, in areas ranging from wearable devices and proprietary sensors, to firmware, data algorithms, online dashboards, and mobile apps.

---

Fitbit’s dedication to health and wellness in the United States goes far beyond selling wearable fitness trackers and smart watches, but these products are the foundation for our continuing efforts to improve Americans’ health and for our future as a company. A 25% tariff would distort competition for wearable devices in the U.S. market and could put this future at risk. Fitbit believes that this tariff would result in a competitive advantage for Chinese device makers in the U.S. market, advance the primary objectives of Chinese industrial policies discussed in USTR’s Section 301 Report, and implicate national security concerns by placing sensitive U.S. health, location, and financial data within the Chinese government’s reach.

tariffs on wearables would adversely affect fitbit and the u.s. economy

The market for wearables, both in the United States and globally, is highly competitive and rapidly evolving. According to Market analyst International Data Corporation (“IDC”), worldwide shipments of wearable devices grew by 55.2% year-over-year in the first quarter of 2019, including 31.6% growth in shipments of wrist-worn wearables.6 IDC expects the global wearables market to reach nearly 220 million units shipped by 2022.7 U.S. brands like Fitbit are currently the strongest players in the U.S. market, but new entrants, including Chinese brands, are emerging and competing aggressively for market share. According to IDC, two of the top three global wearables brands in

7 Smartwatches to Have More than Just Fifteen Minutes of Fame, According to IDC, IDC (Mar. 20, 2018).
the first quarter of 2019 were Chinese companies, Xiaomi and Huawei. These companies were second and third, respectively, by global market share, while Apple and Fitbit were first and fifth. In the first quarter of 2019, Xiaomi captured the largest share of the global market for wrist-worn wearables, with 46.3% year-over-year growth, while Huawei’s share grew by an even larger 213%. U.S. and Chinese brands are thus competing intensely, not only for sales of devices themselves, but also – and perhaps more importantly – for the downstream products and services that the devices support.

To remain competitive in this market for the long term, Fitbit needs to maintain its strong position in the U.S. market. The United States continues to be Fitbit’s most important source of revenue and the primary location of the company’s research and development efforts. From 2015-2017, device shipments to the United States accounted for nearly 70% of Fitbit’s total revenue and were thus a vital source of funding for Fitbit’s R&D efforts and its expansion into new market segments. A 25% tariff on Fitbit’s device imports from China would impose immediate and substantial costs that could compromise Fitbit’s ability to compete in the market for wearable devices in both the consumer and healthcare sectors.

---

These effects would ultimately extend beyond Fitbit. As noted above, Fitbit partners with more than 1,500 U.S. companies in employee wellness programs, relying on Fitbit products to lower healthcare costs and improve employee health. These partners include small and medium companies that may not be able to afford the price increases that would result from these tariffs and may ultimately need to end their participation. For other partners, the increased costs of the products could offset a substantial portion of any savings in healthcare costs. Fitbit’s products are also sold in more than 15,000 retail stores
that employ millions of Americans across the country. In many cases, a lost sale for Fitbit is a lost sale for retailers and their workforce, not to mention a burden on the consumers who purchase Fitbit products at higher prices resulting from the tariffs. These effects could be especially acute if the tariffs were to take effect in the fourth quarter, during the holiday season, when device sales are typically at their strongest. This year, for example, IDC anticipates that one-third of total device shipments will occur in the fourth quarter.

As a result,
The tariffs would therefore cause substantial and possibly irreparable short-term and long-term harm to Fitbit, to its partners – including the U.S. government – in the healthcare and employee wellness space, and to the retailers who sell Fitbit’s products. These effects would ultimately harm U.S. workers and consumers, and they could not be avoided easily by relocating final assembly to the United States or a third country in the foreseeable future. Even if relocating final assembly were a realistic short-term possibility, which it is not, the heavy costs associated with doing so would themselves force Fitbit to raise prices and would therefore not mitigate the likely harm caused by lost market share to low-margin Chinese competitors.

tariffs on wearables would enhance Chinese brands’ competitiveness in the u.s. market, advancing China’s objectives in the big data sector

Competition in the United States from Chinese brands that are expanding rapidly in the global wearables market is a key concern regarding any trade action that will force U.S. companies to raise their prices. China’s major wearables brands, especially Huawei and Xiaomi, compete by operating on
razor-thin profit margins for device sales, with an eye on expanding their user base and generating revenue through downstream products and services. Xiaomi’s model, for example, is to “sell low-priced, high-quality commodity devices at thin margins, then make money by selling ‘internet services,’” like in-house apps embedded in the company’s devices.\textsuperscript{10} Xiaomi’s second wearable fitness tracker, the Mi Band Pulse, entered the market in 2015 at a retail price of only $15.\textsuperscript{11} The company recently stated its intention to cap its profit margin on device sales at 5% in advance of its 2018 IPO.\textsuperscript{12} In its IPO prospectus, Xiaomi repeated its “pledge to our existing and potential users” that “starting in 2018, Xiaomi’s hardware business (including smartphones, IoT and lifestyle products) will have an overall net profit margin that will not exceed 5% per year.”\textsuperscript{13} It added that it “will return the excess above 5% to our users,” while emphasizing that “the sheer amount of unique consumer and behavioral data created by our platform gives us a massive advantage in the field of big data and artificial intelligence.”\textsuperscript{14} Chinese companies like Xiaomi, in other words, appear willing and able to sacrifice profits on device sales simply to capture global market share in a manner that U.S. companies like Fitbit cannot afford.

In addition to this low-margin business model, Fitbit’s Chinese competitors benefit from government support that will allow them to minimize, if

\textsuperscript{10} See, e.g., Josh Horwitz, The Case for Xiaomi, the $70 Billion Company – and for Xiaomi, the $30 billion Company, Quartz (June 4, 2018).

\textsuperscript{11} Jon Russell, Xiaomi’s Second Wearable Device Tracks Your Sleep, Steps and Heart Rate for $15, Tech Crunch (Nov. 9, 2015).

\textsuperscript{12} Yingzhi Yang, Greed is Not Good at Xiaomi, as Founder Caps Profit Margin on Its Hardware Business at 5 Per Cent, South China Morning Post (Apr. 25, 2018).

\textsuperscript{13} Xiaomi Corporation, Global Offering (June 25, 2018) at 219.

\textsuperscript{14} Id. at 215, 219.
not eliminate, the effects of U.S. tariffs on their prices. The Chinese Ministry of Commerce in July 2018, for example, “announced new policies that aim to relieve the impact of China-U.S. trade frictions,” including by “using the income raised by China’s countermeasure tariffs to relieve the impact on affected companies and their employees.” According to a recent report, “Huawei’s annual reports and public records show that it has received hundreds of millions of dollars in grants, heavily subsidized land to build facilities and apartments for loyal employees, bonuses to top engineers, and massive state loans to international customers to fund purchases of Huawei products.” In its IPO prospectus, Xiaomi reports receiving nearly RMB 426 million in government grants over the last three years.

The nature of their business models and the prospect of subsidies from the Chinese government mean that a 25% tariff on imports from China could be more of an opportunity than a deterrent for Chinese wearables brands in the U.S. market. U.S. companies like Fitbit importing their devices from China would need to raise prices and forego investment in U.S.-based innovation, while Chinese companies could ship through the tariff, gain market share, and establish a foothold in the United States. Currently, no major wearables brand manufactures in the United States, while the two leading U.S. brands (Apple and Fitbit) both assemble their devices in China. There is, in other words, no U.S.

15 China Is Ready to Meet the Costs of the Trade War, People’s Daily (July 10, 2018).
17 Xiaomi Corporation, Global Offering (June 25, 2018) at 324.
industry that would benefit from these tariffs, while U.S. companies like Fitbit would incur substantial costs.

Simply put, in a trade action targeting Chinese industrial policies, tariffs on wearable devices would be “friendly fire” that is more likely to benefit Chinese brands at the expense of U.S. companies that the Administration’s response should be designed to protect. Much like Xiaomi’s business model, moreover, the Chinese government’s industrial policies in this sector are not focused on the devices themselves, but on the economic and political leverage to be extracted from the “ecosystem” that the devices unlock when enough users wear them.

Any measure that puts American companies like Fitbit at a disadvantage vis-à-vis Chinese competitors therefore risks backfiring by advancing one of the Chinese government’s most important, long-term objectives under Made in China 2025 and related industrial policies: collecting and utilizing big data to promote development in sectors ranging from basic manufacturing to artificial intelligence, cloud computing, and healthcare. The Economist recently observed that “the world’s most valuable resource is no longer oil, but data.” Others have described a “fourth industrial revolution” that is “characterized by a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres,” with implications for innovation “in fields such as artificial intelligence, robotics, the internet of things, autonomous vehicles, 3-D printing, nanotechnology, biotechnology, materials science, energy storage, and quantum

---

18 The World’s Most Valuable Resource is No Longer Oil, But Data, Economist (May 6, 2017).
The Chinese government is acutely aware of these interconnections and has structured its new generation of high-tech industrial policies with this future in mind.

An important distinction between smart products like wearables and many of the other products that have been included on USTR’s proposed tariff lists is that smart products are the terminals that allow access to a highly interconnected, rapidly evolving “digital ecosystem” of emerging industries, in which American companies are among the world’s strongest competitors. In this context, wearables are important to Chinese industrial policy less as “things” to be sold, and more as a means of achieving an array of other economic and strategic objectives that have broader implications for U.S. innovation, consumer privacy, and national security. China’s industrial policy plans recognize that wearable devices may continuously collect a user’s information, including health data, geolocation information, financial transactions and history, facial and voice recognition, social media usage, and other sensitive data. The 2017 Made in China 2025 Bluebook, for example, discusses developing “representative IT products like smart wearable equipment, unmanned vehicles, and smart service robots,” as a means of “actively promoting the integration of hardware and software, manufacturing and services, and the internet and products.”

Disturbing competitive markets for products like wearables, particularly when

---


20 See, e.g., Mumtaz Ahmed et al., *Where Do You Fit in the New Digital Ecosystem*, Deloitte (2016) at 2 (“The digital ecosystem comprises a vast universe of TMT businesses that provide a broad range of products and services.”).

U.S. brands are the strongest players in those markets, risks hindering U.S. competitiveness and advancing Chinese industrial policy objectives throughout the “ecosystem.”

The Chinese industrial policies highlighted in USTR’s Section 301 report clarify the strategic importance of big data to the government’s development goals. Explaining the context of its publication, the State Council’s Made in China 2025 plan emphasizes that “all countries are expanding their efforts in technological innovation and achieving new breakthroughs in areas including 3-D printing, mobile internet, cloud computing, big data, bio-engineering, new energy, and new materials.” It emphasizes utilizing big data to advance objectives related to integrating informatization and industrialization, including development of big data processing software for industrial applications. The 2017 revision of the Made in China 2025 Priority Technology Roadmap likewise emphasizes that cloud computing, the internet of things, big data, and artificial intelligence are at the core of “a new generation of technological revolution and industrial transformation.” The Internet Plus plan, in turn, references big data 23 times in the context of industrial policy objectives in sectors including artificial intelligence, e-commerce, logistics, and finance, in particular calling for “researching and issuing a national big data strategy, especially for increasing the

23 Id. at § 3(2), 6(1).
country’s ability to control big data.”25 The Chinese government has identified big data as a “basic national strategic resource” and emphasized its significance in both economic and political spheres.26

Characterizing big data as “the 21st century’s iron ore,” a subsequent Development Plan for Big Data Industry (2016-2020) issued by the Ministry of Industry and Information Technology (“MIIT”) reveals the Chinese government’s view of big data as any other raw material to be extracted and consumed for downstream applications of strategic importance to the state.27 This implicates an array of privacy and national security concerns. As with similarly structured industrial policies in other sectors, China intends to develop several large, national champion enterprises on a global scale, and to deploy data throughout the economy to advance cross-cutting national objectives.28 The government intends to “promote combined big data innovation across sectors,” suggesting a communal approach in which data collected by strategic enterprises effectively becomes centrally administered state property that may be freely accessed and utilized to the extent that it serves official objectives. Referencing the IT, energy, financial, trade, agriculture, food processing, culture, and public


28 Big Data Industry Development Plan at 7-8.
security spheres, the *Big Data Industry Development Plan* aims to “promote the collection, consolidation, sharing, and application of big data resources to fully liberate the transformative role of big data in industrial development.”

In August, both Huawei and Xiaomi were included in a list of the 2018 “Top 50 Chinese Big Data Enterprises” identified by the state-affiliated Big Data Industry Alliance of China, suggesting that they will be important players in China’s strategic objectives in the big data space.

As a “national strategic resource,” in other words, big data in China is the province of the state, to be collected, consolidated, shared, and applied, with implications both for emerging technologies like artificial intelligence and cloud computing, and for national security. While *Made in China 2025* refers to smart wearables as one product within the basket of “smart manufacturing equipment and products,” they are discussed in greater detail elsewhere as a means of collecting the data that is vital to China’s more expansive development strategies. “Smart terminals,” including wearables, are thus the excavation equipment that is necessary to harvest the “national strategic resource” of big data. With regard to a corner of the “digital ecosystem” that is particularly relevant to Fitbit, the 2016 edition of the China Academy of Information and Communications Technology’s (“CAICT”) *Big Data White Paper* notes that “wearable equipment is capable of collecting individual health data on an uninterrupted, 24x7 basis,

---

29 Id. at 13.
31 Guo Fa (2015) No. 28 at § 3(2).
32 See, e.g., MIC 2025 Roadmap at 3 (identifying “mobile smart terminals”).
with broad-ranging potential applications in the healthcare sector.” This data is vital not only for insurers and service providers like the ones that rely on Fitbit’s products, but also for developing next-generation medical device technology based on artificial intelligence capabilities. Unlike wearables, these devices are a direct concern of the Made in China 2025 plan. The Roadmap states objectives including building and administering a health database and promoting greater competition in international markets by Chinese medical device brands.  

Tariffs that distort the competitive landscape in a manner that could favor Chinese wearable brands in the U.S. market at the expense of U.S. brands would thus be more likely to advance Chinese industrial policy goals that are far more important to the government’s long-term technology strategies than assembling wearable devices. A significant loss of U.S. market share to Chinese competitors would in fact be similar to a direct Chinese acquisition of Fitbit’s database in terms of the national security implications. The Chinese government could use access to valuable U.S. user data to advance its objectives throughout the “digital ecosystem,” from e-commerce to artificial intelligence to medical device technology. The adverse effects of this could extend well beyond economic competition and implicate U.S. national security in a manner that would likely trigger mandatory CFIUS review under new rules regarding critical technologies if accomplished by way of direct investment or acquisition.

---

34 MIC 2025 Roadmap at 284-285.
tariffs on wearables would implicate national security, political, and privacy concerns

The Chinese government’s plans for big data technologies are not only economic. They are political (and geopolitical). According to a recent study, “No government has a more ambitious and far-reaching plan to harness the power of data to change the way it governs than the Chinese government.”35 Through its centralized data collection and management strategies, the Chinese government “is thoroughly reshaping its approach to economic and social governance” in a way that potentially “presents a fundamental challenge to democratic political systems.”36 By giving Chinese brands a competitive advantage in the U.S. market, a 25% tariff on wearables could give the Chinese government access to a wealth of sensitive personal information of Americans and inadvertently further these objectives in unforeseeable ways. The Administration has already recognized the potential national security concerns surrounding Chinese technology by adding Huawei to the Bureau of Industry and Security’s “entities list” and proposing bans on the use of technology, including 5G network equipment, supplied by companies subject to the jurisdiction of “foreign adversaries.”37

The most prominent example of the Chinese government’s approach to political control is the introduction of a “social credit system” in 2014, through

35 Martin Chorzempa et al., China’s Social Credit System: A Mark of Progress or a Threat to Privacy?, Peterson Institute for International Economics (June 2018) at 1.
36 Sebastian Heilmann, Big Data Reshapes China’s Approach to Governance, Financial Times (Sept. 28, 2017).
37 Trump Has Banned Telecoms Equipment from “Foreign Adversaries”, MIT Technology Review (May 16, 2019).
which the government aims to compile a massive database and, by 2020, assign “every individual . . . a social credit score” that reflects “a wide range of information, including financial data, criminal records, traffic violations, social media activity, and consumer purchases.”

The system has been characterized as “part of the Chinese government’s ongoing efforts to counter perceived threats and shape citizens’ behavior through massive data-gathering and surveillance.”

In addition, the government has deployed an extensive surveillance system based on facial recognition data known as “Sky Net,” which, according to Chinese media “can scan China’s population in a second” with 99.8% accuracy.

According to one recent study,

Chinese public security forces are emerging as a powerful and dominant intelligence and security sector. The interest from the public security forces in using big data to support government systems for faster and more extensive surveillance and social control largely explains the rapid rise of China’s big data industries. Private companies are . . . sharing users’ personal data with the authorities in compliance with China’s Cybersecurity law, the National Intelligence Law, and other relevant internet management regulations . . . .

The aggregation of data and the use of artificial intelligence have been central to Chinese authorities’ tracking and detention of ethnic minorities deemed to be threats to political stability across the country, including in the Xinjiang

---


39 Id.


Autonomous Region. A recent report by Human Rights Watch details “a mobile app that police and other officials use to communicate with the Integrated Joint Operations Platform,” that “aggregates data about people and flags to officials those it deems potentially threatening; some of those targeted are detained and sent to political education camps and other facilities.” With access to foreign user data, tools such as these could be deployed globally to, for example, monitor the movements and activities of persons of political and strategic interest abroad, including in the United States.

China’s goals with respect to collecting and utilizing data for political objectives extend beyond its own borders. One goal of the social credit system plan is “improving the country’s soft power and international influence,” including “protecting the CCP and securing the ideological space both inside and outside the party. That task transcends geographical borders.” The legal authority for recent pressure that the Chinese government applied to foreign airlines with respect to their identification of Taiwan as a “country,” for example, was a regulation issued to implement certain guidelines under the social credit

---

42 See, e.g., Paul Mozur, One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority, New York Times (Apr. 14, 2019); Zak Doffman, China is Using Facial Recognition to Track Ethnic Minorities, Even in Beijing, Forbes (May 3, 2019).


44 Owen Churchill, Chinese Communist Party is Stepping Up Efforts to Stifle Dissent Abroad, U.S. Officials are Told, South China Morning Post (Aug. 25, 2018) (“China’s ruling Communist Party is pursuing an aggressive, covert infiltration of U.S. educational and social institutions to quell dissenting voices and strengthen its soft power overseas . . . .”).

system framework. The Chinese plans to create a “digital silk road” under the auspices of the “One Belt, One Road” initiative also “have raised concerns that Beijing could use those networks to exert pressure on other states or engage in electronic surveillance.” The Chinese government has even suggested using concepts drawn from the Internet Plus plan to organize overseas political influence activities among individuals abroad by utilizing big data in United Front work efforts. One article explains recent experiments with a “big data + United Front” strategy to improve United Front recruiting and monitoring efforts.

Finally, the Chinese government has emphasized the importance of big data and artificial intelligence in its military planning objectives. In recent testimony before the U.S.-China Economic and Security Review Commission, one expert highlighted China’s “implementation of a strategy of military-civil fusion in artificial intelligence,” and its calls “for strengthening the use of AI in military applications that include command decision-making, military deductions

46 Id.
47 Nyshka Chandran, Surveillance Fears Cloud China’s ‘Digital Silk Road,” Yahoo Finance (July 11, 2018).
48 Use More Online Thinking in United Front Work (让统战工作多些互联网思维), Xinhua (May 8, 2018). See also Philip Wen, China Strengthens Global Influence Agency in Government Reshuffle, Reuters (Mar. 21, 2018) (noting that “[t]he activities of the United Front Work Department . . . have drawn greater scrutiny over the past year in democracies such as Australia and the United States, whose governments have expressed concern over Chinese efforts to influence their political processes . . . .”); Alexander Bowe, China’s Overseas United Front Work, U.S.-China Economic and Security Review Comm’n (Aug. 24, 2018).
(e.g., wargaming), and defense equipment.”\textsuperscript{50} This includes “urging the advancement {of} the application of big data, cloud computing, artificial intelligence, and other cutting-edge technologies to the construction of the {People’s Liberation Army’s} command system for joint operations,” in pursuit of a broader drive to “{a}ccelerate the development of military intelligentization . . .”\textsuperscript{51}

In addition to tracking sensitive individual health data, wearable devices increasingly include advanced features and functionality related to facial and voice recognition, e-payment and financial networks, geolocation, access control for mass transit systems and smart locks, and always-on microphones. The capacity of these devices to collect sensitive data on a 24x7 basis has the potential to exceed that of smart phones. In the hands of companies closely linked to a foreign government with a broad array of strategic and political objectives tied to exploiting big data, this information could have serious implications for U.S. national security and the privacy of U.S. citizens. This includes U.S. military and law enforcement personnel. Fitbit stores its data solely on servers in the United States, subject to strict privacy protection rules and security safeguards. But there is very little preventing the same data collected by Chinese companies from ending up on Chinese servers, where it may be shared with or accessed by authorities pursuing the industrial policy and political objectives discussed above.

\textsuperscript{50} Elsa B. Kania, \textit{Testimony Before the U.S.-China Economic and Security Review Commission Hearing on Trade, Technology, and Military-Civil Fusion: Chinese Military Innovation in Artificial Intelligence} (June 7, 2019) at 3.

\textsuperscript{51} \textit{Id.}
As noted above, Huawei is one of China’s foremost competitors in the global wearables market. In February 2018, U.S. intelligence and federal law enforcement officials testified before the Senate Intelligence Committee and highlighted concerns regarding American use of devices and equipment made by Huawei and ZTE, another Chinese manufacturer of mobile devices, including wearables. FBI director Christopher Wray explained that the Bureau is “deeply concerned about the risks of allowing any company or entity that is beholden to foreign governments that don’t share our values to gain positions of power inside our telecommunications networks.”

Concerns arise not only from the devices themselves, but also the potential vulnerabilities embedded in any third-party software installed on the devices. In late 2017 and early 2018, fitness tracking software distributed by Strava revealed the location of classified U.S. military installations by way of shared movement and location data of official personnel, raising concerns about U.S. national security. Recent reports reveal that Huawei has actively mined the data collected by third-party chat and social media software installed on its devices, in part to develop its own next-generation artificial intelligence technologies. Ultimately, sensitive data collected by wearables could be accessed by Chinese authorities under the Cybersecurity or National Intelligence laws to identify and surveil individuals of interest to the Chinese intelligence or

52 Sara Salinas, Six Top U.S. Intelligence Chiefs Caution Against Buying Huawei Phones, CNBC (Feb. 13, 2018).
public security apparatus. Recently amended changes to Xiaomi’s U.S. privacy policy suggest that the company will begin collecting “personal information including driving license and passport details along with financial information like bank account and credit card number(s)” from its users in the United States.\textsuperscript{55} The privacy policy explicitly states that Xiaomi is headquartered in China and may store data at data centers in multiple countries, including China and Russia.

For now, Chinese wearables brands do not have a dominant footprint in the U.S. market, but a 25% tariff that would force U.S. brands to raise prices would likely change that dynamic by playing into the low-margin strategies that Chinese brands have adopted in competing for global market share. Upsetting the competitive landscape in this manner would give Chinese brands an advantage over U.S. brands, with far-reaching effects that extend beyond commercial competition and implicate the privacy of U.S. citizens and even U.S. national security.

\textbf{tariffs on wearables would not advance the administration’s policy objectives}

Fitbit submits that it is not worth risking any of the negative consequences discussed above when a 25% tariff on wearable device imports would not address the concerns highlighted in USTR’s Section 301 Report. The report addresses certain acts, policies, and practices that “work collectively as part of a multi-faceted strategy to advance China’s industrial policy objectives.”

through “the acquisition of foreign technologies.” The report specifically emphasizes:

- The use of foreign investment restrictions and related administrative approval requirements to pressure technology transfer;

- Government pressure on foreign companies to license technology in China on non-commercial terms;

- State-directed investments and acquisitions of foreign companies to acquire strategic technologies;

- State-backed cyber intrusions or other unauthorized access to commercial secrets or other proprietary information; and

- Other acts, including undue pressure applied to foreign companies under the pretense of national security, anti-monopoly enforcement, or standardization requirements.

Fitbit’s Chinese assembly operations have not been subjected to any of these acts, policies, or practices. Fitbit uses contract facilities for final assembly of its products in China, and these arrangements do not implicate any ownership or investment restrictions, or any licensing or approval processes that create pressure to transfer technology into Chinese control. Fitbit has not been the object of any proposed investments or acquisitions by any Chinese company, and it has no plans to consider any such transactions in the foreseeable future. Fitbit has not been targeted by cyber intrusions or other unauthorized access to confidential business information by Chinese entities. Finally, Fitbit has not experienced any pressure from Chinese authorities related to national or cybersecurity laws or regulations, competition law enforcement, standardization

---


57 Id. at 17-18.
laws, or talent acquisition. Fitbit remains firmly in control of its proprietary technologies and commercial secrets and has no reason to believe that this intellectual property will be compromised by its use of assembly partners in China.

Because neither Fitbit nor Fitbit’s technologies have been targeted by the acts, policies, and practices highlighted in USTR’s Section 301 Report, tariffs on wearables would not advance the Administration’s policy objectives. As discussed above, however, tariffs would disproportionately affect U.S. companies like Fitbit and harm the U.S. economy, while compromising U.S. national security interests and advancing the Chinese government’s broader industrial policy objectives by making Chinese brands even more competitive in the U.S. market.

**Conclusion**

For these reasons, Fitbit respectfully requests that USTR remove HTSUS subheading 8517.62.0090 from the list of tariff lines potentially subject to 25% tariffs under the May 17, 2019 *Proposed Modification of Action*. Alternatively, Fitbit requests removal of wearable devices such as fitness trackers and smart watches. At the very least, USTR should delay implementation of the tariffs with respect to these products pending further consideration of the issues raised herein. As discussed above, a 25% tariff on these products would adversely affect U.S. companies like Fitbit and give Chinese brands like Huawei and Xiaomi a competitive advantage in the U.S. market. This would advance Chinese industrial policy objectives and implicate U.S. privacy and national
security concerns without addressing the acts, policies, and practices highlighted in USTR’s Section 301 Report.

* * *

Fitbit, Inc. requests that certain information contained in square brackets (“[ ]”) throughout this submission, specifically on pages 6-9, be protected as business confidential information. Fitbit certifies that disclosure of the information in square brackets throughout this submission would endanger trade secrets and profitability, and this information would not customarily be released to the public. Fitbit is concurrently filing a public version of this submission.

Respectfully submitted,

Andy Missan

Executive Vice President & General Counsel
Fitbit, Inc.