U.S. HOUSE OF REPRESENTATIVES (118th CONGRESS)

COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY, AND THE INTERNET

IP and Strategic Competition with China: Part IV – Patents, Standards, and Lawfare

Kent D. Baker
Head of IP Strategy, Litigation, Standards & Licensing
u-blox America, Inc., Intellectual Property & Standards

Written Testimony

December 18, 2024

Mr. Chairman and distinguished members of the Committee, my name is Kent Baker, and I am the Head of IP Strategy, Litigation, Standards and Licensing at u-blox America, Inc. (ublox). ublox, founded in 1997, provides wireless semiconductor chips, modules[1], and Internet-of-Things (IoT) services that reliably locate and connect everything-to-everything. We build components, not end products, and do not sell our chipsets to third parties. The component technologies include satellite, cellular, WiFi, Bluetooth, and other wireless tech. ublox cutting-edge solutions drive innovation for the car of the future and IoT connectivity while employing over 1000 experts who enable our customers to build wireless solutions for a precise, smart, and sustainable future. Our customers manufacture products used in Smart Cities, gas and water meters, medical devices, robotics, security systems, tracking devices such as shipping containers, dog collars and industrial equipment, and even

[1] Generally, there is a semiconductor chipset inside a module and the module is integrated into a modem. A module may be used for a wireless connection or embedded with modem features.

The **chipset** conducts several basic wireless connection functions. It negotiates the lowest levels of connection with the wireless network. Basically, it controls all the super nerdy radio-frequency (RF) stuff that is required to connect and communicate data, text, or voice over the wireless connection. It cannot connect to the internet or any other wireless network without other supporting things like antennas, filters, etc. For an end product manufacturer, this is very complicated to build and not cost effective to design. Specialty design companies such as Qualcomm provide chipsets.

The **module** will typically have the chipset, a small processor, some memory, and some voltage regulation stuff. Cellular alone or some additional wireless functionality such as GPS/GNSS systems may be included. A module board is a most basic way to connect an IoT device to the Internet via a wireless connection and is used extensively in IoT devices. This is the thing that "talks" to the cellular base station or other wireless network such as a satellite, router, etc.

The **modem** implements the module, which in turn contains the chipset. The modem offers a simpler overall hardware setup that's easier with which to work and may integrate other features for more complex product uses, for example, sensors of various types.

"driverless" lawn mowers, to name a few. Since the modules are physically small and embedded inside larger devices, the module presence goes unnoticed and overlooked as do issues regarding the emerging Chinese module dominance and security concerns. For 2024, ublox revenue is expected to reach approximately $240 million. ublox maintains a small but essential patent portfolio and is a patent licensee (user).

The ublox experience with standard essential patents (SEPs) and Chinese competitors comes from practical experience moored in market realities as a small/medium sized company. The experience springs from "in-the-trenches" business and license dealings involving SEPs and the SEP valuation principle of fair, reasonable, and non-discriminatory (FRAND) to which every standards member agrees to abide.

Prior to joining ublox in 2017, I started my career as a prosecutor which I left to join an established patent and trademark law firm. This time was followed by many years at Qualcomm, Inc., as Vice President-Division IP Counsel, and at the Palo Alto Research Center (PARC) Xerox, a prolific and storied innovation hub spanning numerous technology sectors and leading to the creation of startup companies.[2] I am a named inventor on one patent, a registered patent attorney, and have degrees in engineering, material science, law, and business.

[2] The ethernet and numerous other life-changing technologies, as well as Apple and other companies, were built off the back of PARC technical innovations, an amazing innovation hub dating to the 1970s. "Dealers of Lightening: XEROX PARC and the Dawn of the Computer Age," Michael Hiltzik (1999), ISBN 0-88730-891-0

Throughout my career and as wireless technology grew from infancy, I have been intimately involved in global standardization policy issues concerning wireless connectivity and video/audio coding. In this role, I have discussed IP policy with government officials including the European Union, China, Brazil, Vietnam, India, and others. I conjointly worked on the International Telecommunication Union (ITU)[3] TSB Director's Ad Hoc Group's "*IPR Intellectual Property Policy and Guidelines*", the ETSI[4] "*Guide on Intellectual Property Rights (IPRs)*", and the ABA "*Standards Development Patent Policy Manual*"[5], the American National Standards Institute (ANSI) Intellectual Property Rights Policy Advisory Group, and the Telecommunications Industry Association's "*TIA Intellectual Property Rights Policy,* " and to the extent possible, at the China Communications Standards Association (CCSA).[6] My work has also included theoretical and practical studies on SEP patent identification and economic valuation principles, and I have authored a paper on the fallacies of comparable license valuation for SEPs. I thank you for the opportunity to testify before you today.

[3] *ITU* is a specialized agency of the United Nations. See, https://www.itu.int/en/ITU-T/ipr/Pages/adhoc.aspx .

[2] *European Telecommunications Standards Institute* (ETSI) is an independent, not-for-profit, standardization organization operating in the field of information and communications. ETSI supports the development and testing of global technical standards.

[5] *American Bar Association*; Committee on Technical Standardization, Section of Science & Technology Law (2007), ISBN-978-1-59031-928-4.

[6] CCSA is a Chinese professional standards organization with the responsibility for developing communications technology standards for the People's Republic of China (PRC).

Module Security

Many nations including the United States are slowly appreciating the threat posed by Chinese company involvement in their telecommunications networks and to the importance of maintaining the lead in semiconductors and wireless IoT modules.[7] *However, the Huawei and ZTE security concerns in wireless communication networks and mobile devices were the tip of the iceberg.* There is much less awareness of the risks incurred by using Chinese cellular IoT modules and technology in existing cellular and other wireless networks. In the short and longer term, the risk posed by the pervasive and fast-growing presence of Chinese cellular IoT modules in U.S. networks poses a greater threat than did relying upon Chinese companies to supply 5G base stations and mobile devices.[8] As Chinese manufacturers dominate the global supply of wireless modules, specifically cellular IoT modules, the module industry recognized the threat and sounded alarms about what the potential threat could pose for all nations.[9] The problem can be framed as a Chinese cellular module having the embedded capability to remotely receive firmware updates without the end-user knowing, thereby allowing settings to be

[7] The US-China Economic and Security Review Commission's 2018 report to Congress claimed that significant state support for these wireless technologies have helped China to achieve dominance in the manufacturing of "global network equipment, information technology, and IoT devices."

[8] Federal Communications Commission bans equipment authorizations for Chinese telecommunications and video surveillance equipment deemed to pose a threat to national security pursuant to the Secure Equipment Act of 2021. *https://docs.fcc.gov/public/attachments/DOC-389524A1.pdf*

[9] Gokhale, Nitin A. (March 2024). https://stratnewsglobal.com/the-gist/india-well-aware-of-the-cellular-iot-module-threats/

manipulated.[10] A fast-growing concern, firmware updates are known to contain malware which can enable a supplier to remotely control a device, access the network, steal unlimited amounts of data to track users and user behavior, or even shut the device or network down entirely.[11] Similar to base stations and mobile devices, the module presents a network security vulnerability. It has further been reported that the Chinese Communist Party (CCP) supports its domestic companies in global sales by providing subsidies worth hundreds of millions of dollars with the aim of controlling the market.

Module companies based in the West see major national security threats from a Chinese monopoly over cellular modules as emerging in three ways. One, the monopoly will allow CCP to pressure dependent countries to modify their policies according to CCP interests or risk module supplies being cut off. Two, through malware designed as module firmware updates, CCP can sabotage large-scale critical infrastructures like power grids, water systems, supply chains, robotics and production lines plus more. And last, modules can be used as gateways to hack into large amounts of private data. The data

[10] It should be noted that the House Select Committee on the Chinese Communist Party has already raised concerns over the close links between the top cellular module manufacturer Quectel and the Chinese military-industrial complex. The Committee wrote to the Federal Communications Commission (FCC), warning of security risks posed by Chinese-made modules such as those made by Quectel, especially in IoT devices used by law enforcement or in vital industries such as electricity generation or water and sewage. Waterman, Shaun and Tatlow, Didi. (January 2024). *Lawmakers to Biden Administration: Sanction Chinese Internet Device Company.*
Also see, *Newsweek*, (April 2024), https://www.newsweek.com/china-sanctions-iot-modules-manufacturer-quectel-gallagher-defense-treasury-1858324

[11] Altavilla, Dave. (September 2023). *Securing The IoT From The Threat China Poses To US Infrastructure*. *Forbes*. https://www.forbes.com/sites/davealtavilla/2023/09/03/securing-the-iot-from-the-threat-china-poses-to-us-infrastructure/?sh=6d2a8c812c0b .

collected from devices can be effectively used for many nefarious tasks, such as threatening key individuals or businesses, and also studying the behavior and location of U.S. citizens, both individually and in bulk.

Further, US and Western industry positions unintentionally shield the nature of the threat arising out of the growing Chinese monopoly over wireless modules. While there is a growing awareness regarding the nature of the threat, there is also a reluctance from module implementors and industry players to recognize the issue due to questionable and uninformed fears that addressing the issue may lead to short-term disruption in the supply of low-cost modules and thereby impact profits.[12] Many reputed Western companies are known to use Chinese-manufactured modules.[13]

So, what should be done?

- Spread awareness among private and government users regarding the nature of the threat posed by Chinese-manufactured modules.
- Encourage procurement of wireless modules only through trusted channels, and compile a list of untrustworthy Chinese suppliers, and ban the supply of such modules into the United States.

[12] Parton, Charles. (March 2024). *Chinese cellular (IoT) modules: Countering the threat.* Council on Geostrategy. https://www.geostrategy.org.uk/research/chinese-cellular-iot-modules-countering-the-threat/

[13] Drew, Alexi. (August 2022). Chinese technology in the 'Internet of Things' poses a new threat to the west. *Financial Times*. https://www.ft.com/content/cd81e231-a8d3-4bc0-820a-13f525a76117 .

- Pass legislation or implement administrative measures to prevent the purchase of new Chinese IoT modules for domestic products and services with a deadline for compliance.
- Any Chinese-manufactured modules should be prohibited by end 2025 or as soon as possible thereafter from being used in critical sectors like security, health, food supply, water, power, and energy sectors.
- Indigenous production of wireless modules – not just chipsets - should be encouraged and incentivized.
- Collaborate with like-minded nations to address similar concerns and explore joint solutions to reduce dependency on Chinese-origin components.
- Conduct an audit of Chinese modules embedded in government devices, properties and services, and in critical national infrastructure, in order to measure the extent of potential risk and to prioritize areas of greatest risk.
- Require government departments to produce plans to mitigate the risks identified in their agencies.

Chinese Companies Are Winning the Module Market Competition

Three Chinese companies already own over 50% of the international market for cellular IoT modules and exceed 60% for the U.S. market. This international market percentage includes the large Chinese domestic market which is

mostly unavailable to Western suppliers. Chinese Communist Party policy documents show the strategic importance of IoT technology to the CCP.[14] In line with CCP industrial policy to promote global champions in new industries, Chinese IoT companies have benefited from the creation of a domestic market which excludes meaningful international competition by Western companies, sets preferential pricing regimes for Chinese manufactured products, and provides access to subsidies and centralized funding to Chinese companies. The risk is that as Chinese companies continue to increase global market share to edge out foreign companies, coupled to Chinese policy structured to exclude in-China market competition, China is the largest benefactor of the cellular IoT module market while presenting security risks to democratic countries. Given the immense importance of these modules to modern industry and life, this would also make other countries highly vulnerable to the Chinese module threat.

[14] In 2009, the Chinese government initially designated IoT as a strategic sector for development and followed with significant financial support toward the sectors' development. In 2012 the Ministry of Industry and Information Technology (MIIT) referred to the IoT as a "strategic high ground". In the 13th Five Year Plan, which covered 2016-20, the section on digital and telecoms development included direct efforts aimed at boosting IoT chip design and manufacturing. This was also in support of "information flow" along the Belt and Road Initiative (BRI). This continued in the 14th Five Year Plan. The development of the IoT was intended to support a range of industries including agriculture, city infrastructure, customs and border posts, and manufacturing. See: https://www.uscc.gov/sites/default/files/Research/SOSi_China's%20Internet%20of%20Things.pdf; https://merics.org/en/report/connection-everything-china-and-internet-things. The IoT also appears frequently in the 13th Five Year Plan. In special column 9, it talks of '2. Expansion of the internet of things: We will establish infrastructure for application of the internet of things and service platforms, and promote the creation of important demonstration projects for the application of the internet of things. We will broadly develop the integrated application of the internet of things as well as development of innovative models, and enrich services related to the internet of things.' *See also*, Patton, Charles (2024) "Cellular IoT modules – Supply Chain Security," s*ignificant technical expertise has been provided by Dr. Samantha Hoffman*.

In 2020, Chinese cellular IoT modules were beginning to dominate global markets. (Figure 1.) Combined, Chinese cellular IoT companies represented approximately 50% of the market with the remaining 50% being Western suppliers. A closer look shows Quectel dominance with another Chinese module supplier, Sunsea, moving into second position with an increase in its market share following a 29% Quarter-over-Quarter growth.[15] Fibocom, another fast-growing Chinese vendor, became the third-largest IoT module supplier in Q2 2020 in terms of shipments, surpassing the incumbents Thales, Sierra Wireless and Telit. Fibocom also acquired Western module supplier Sierra Wireless's automotive embedded module business in 2020 with the expectation it would further boost its market share.

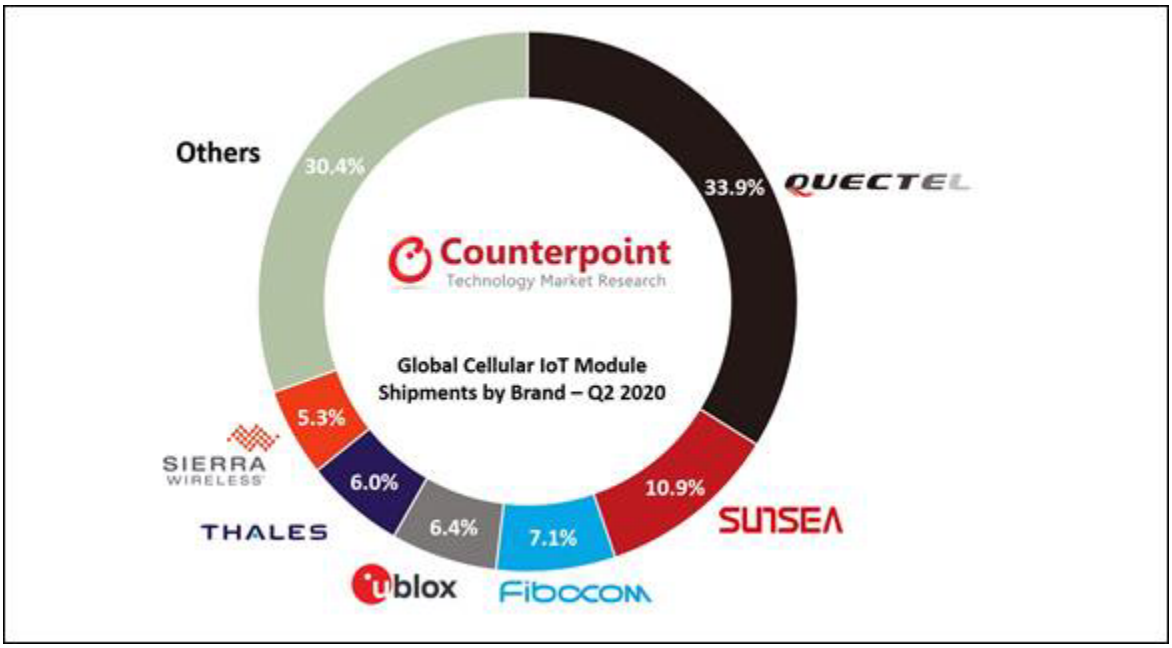


Figure 1

[15] During this time period, it is believed Sunsea group reduced prices to capture additional market share.

Turning to 2024, four years later it is clear the Chinese cellular IoT module market share growth effort was successful. (Figure 2.) Quectel increased its total market share to 36.5% with U.S. market share exceeding 50% as Western suppliers struggle due to unexplainable price reductions.[16] Fibocom market share grew to 7.5% as other Chinese cellular IoT module manufacturers also grew their shares representing in Q2 2024 approximately 65% of the global market. Not one Western cellular IoT module manufacturer made the top five in total global cellular module shipments, and market share in Western countries is also falling at an alarming rate.

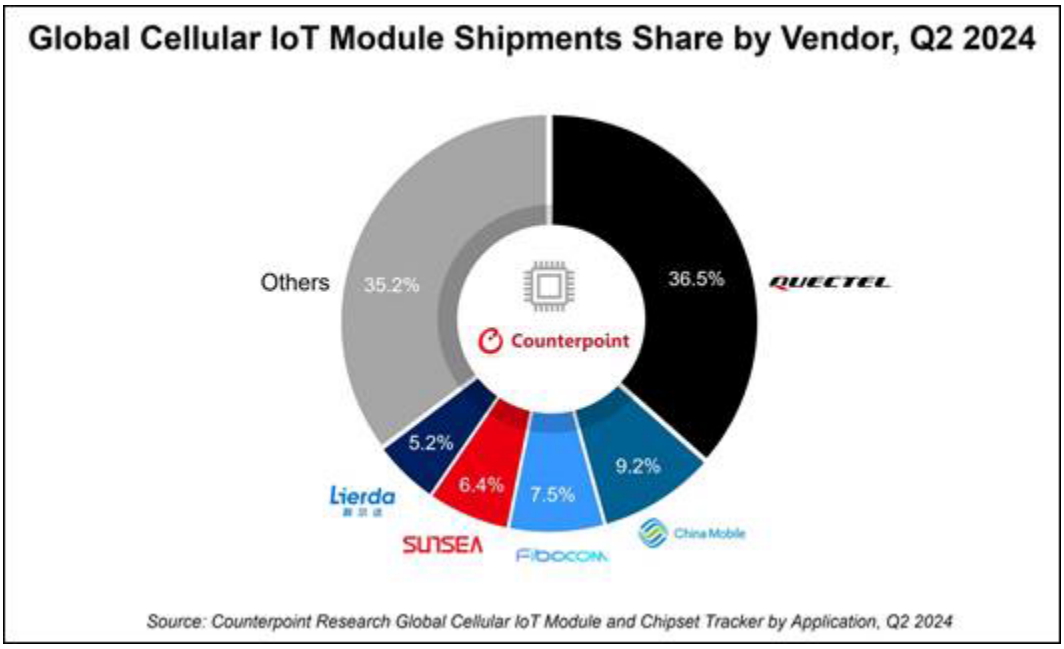
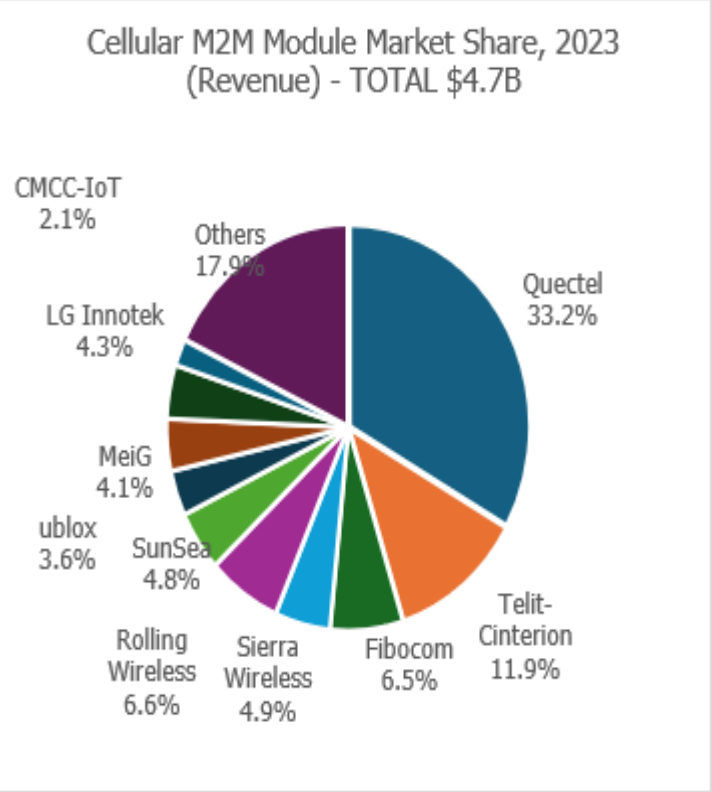


Figure 2

[16] Materials cost for manufacturing a cellular module are commoditized in normal markets. When a comparable cellular IoT module is offered by ublox at $10/unit and a Chinese supplier offers a substantially similar product for $7.50/unit, the cost difference is not reasonably attributable to variables in COGs for manufacture.

Focusing on revenues in one of the fastest growing market segments of the cellular IoT market, Machine-to-Machine (M2M)[17], it is readily apparent that Chinese cellular IoT companies are reaping an increased benefit as Western cellular IoT module manufacturers lose sales. (Figure 3). The total market revenue for M2M IoT uses was $4.7 billion dollars with Western cellular M2M module manufacturers capturing approximately a 30% share of the total market. While the 2023 revenue share for M2M alone is of great concern, the year-over-year volume and revenue growth attributable to Chinese cellular IoT module manufacturers *in toto* far exceeds the revenues generated by higher security, Western designed and supplied module manufacturers. Looking to



[17] M2M refers to direct communications between devices without human intervention. M2M IoT provides quicker and easier connectivity while using less power.[5] to increasingly realize the value of connecting geographically dispersed people, devices, sensors and machines. M2M includes smart cities/municipalities,, smart homes, remote medicine, fleet management, industrial automation, sensors or meters transmitting data to adjust industrial processes, fault detection for industrial robots in dynamic operating conditions such as medical and automotive, personal appliance connectivity, oil and gas system real-time operational data, precision agriculture, military, government, manufacturing, and many, many others. These networks also allow new business opportunities for consumers and suppliers. *How Machine-to-Machine Communication Works*, (2008), https://computer.howstuffworks.com/m2m-communication.htm .

Figure 4, it shows the 2019-2023 volumes in millions of units and revenues in millions of dollars for the three largest Chinese cellular IoT module vendors. Market share percentages reflect the potential to generate revues in the fast growing IoT market, however, revenue growth should be examined when it is understood that module prices tend to decline each year. In 4 years, the top Chinese manufacturer, Quectel, increased revenues from this IoT module segment by 230% which was also reflected in a large increase for Quectel in U.S. market share. Western manufacturers continue to experience year-over-year revenue decreases with no end in sight.[18] The main takeaway is that Chinese module manufacturers

		2019	2020	2021	2022	2023
Quectel	**Volume**	**71.5**	**106.2**	**160.0**	**175.3**	**164.0**
	Revenue	**536.7**	**762.7**	**1,582.5**	**1,797.5**	**1,570.0**
SunSea	**Volume**	**32.0**	**27.5**	**36.0**	**27.5**	**30.0**
(SIMCom/Longsung)	**Revenue**	**209.5**	**177.7**	**289.1**	**215.0**	**228.0**
Fibocom	**Volume**	**11.9**	**21.0**	**27.9**	**21.9**	**28.0**
	Revenue	**141.8**	**207.6**	**234.4**	**271.2**	**307.0**

Figure 4

[18] It is generally understood that avoidance of intellectual property costs is a widespread practice with regard to many participants in the M2M module market. This places a Western manufacturer such as ublox that respects patent rights and pays patent royalties at a significant competitive disadvantage, a result never desired by standards patent policies applicable to SEP use.

aggressively are taking market share at the expense of Western competitors Telit, Thales, ublox, and Sierra Wireless.[19] Note that Telit and Thales had a combined 20.7% market share in 2020 and that is down to 11.9% in 2023 with Sierra Wireless falling from 6.4% to 4.9% share.

The security and competition issues alone should be of great concern to this committee. But even more concerning is the ever increasing participation of Chinese companies at standards organizations' engineering work groups[20], and the current abuses of SEP licensing practices, making it impossible for a Western component manufacturer like ublox to guarantee its customers enjoy patent protection for their essential wireless connectivity needs while also assuring that a patent holder receives FRAND-based compensation for the use of its SEPs by all ublox customers.[21]

[19] Thales and Telit module groups combined to form a new company, Telit-Cinterion based in Irvine, California, and the Sierra Wireless non-automotive module group was acquired by Semtech based in Camarillo, California.

[20] While not perfectly linear, there is strong correlation between the number of company engineers/technicians participating at a standard organization's technical workgroup and patents filed/received based upon that work. This is discussed, *infra*.

[21] Companies participating at standards organizations generally are required to make a minimum commitment to negotiate a license for SEPs it owns with any company that requests a license. (See, ETSI, *Guide on Intellectual Property Rights (IPRs)* and ETSI Intellectual Rights Policy, RULES OF PROCEDURE, 29-30 November 2022, https://www.etsi.org/images/files/IPR/etsi-ipr-policy.pdf

Chinese Company Standards Participation

It should be no surprise that as Chinese companies entered the global markets, it was learned that participation and leadership at various standards bodies was essential to achieving the CCP industrial policy to promote global champions in new industries such as IoT.[22] Over the past twenty years, Chinese companies such as ZTE have deployed patents in more than 55 countries by the end of 2020, the company had filed over 80,000 global patent applications, had about 36,000 granted patents worldwide, with over 4,270 patents being chipset/module patent applications.[23] Huawei numbers follow similar trends as do other Chinese tech companies.

In addition, Chinese companies are major contributors and participants in technology research and standard development in the global 5G arena, pairing Chinese leadership with Western leadership. Chinese companies have achieved breakthroughs in leadership positions at 3GPP, the most important communications standard organization in the world, using a "dual chairmanship" configuration. Chinese companies are commonly members of more than 70 international standardization organizations including ITU, 3GPP, ETSI, IEEE, NGMN and CCSA, and Chinese companies also serve as board members in GSA, ETSI and other standards organizations. To date, numerous Chinese experts serve as chairpersons and rapporteurs in major international

[22] "We will broadly develop the integrated application of the internet of things as well as development of innovative models, and enrich services related to the internet of things." (*See*, fn. 13, *supra*.)

[23] *ZTE ranks global top 3 for sustainable leadership in 5G declared Standard-Essential Patents to ETSI* , https://www.zte.com.cn/global/about/news/20210302e1.html. *See also*, "Who is leading the 5G patent race?" published on February 16, 2021, by IPlytics, a market intelligence company analyzing technology trends, market developments and a company's competitive position.

standardization organizations across the globe. The Chinese companies have submitted since year 2000 in excess of 100,000 research papers and standardization proposals. These research papers and proposals form the invention disclosures that are the backbone of securing a patent for a technical submission. Placing this in relative terms, whereas in 2000 a standards engineering work group – the group that does the heavy lifting of technical advancement that generates patents - would have perhaps one or two engineers from Chinese companies. Currently, engineers from Chinese companies participating at standards work and policy groups has grown significantly.

Understanding the growing participation of Chinese companies at global standards organizations helps to understand how Chinese companies couple ever-growing standards participation to fuel patent filings and build massive SEP patent portfolios that are then not offered on FRAND terms and conditions.

The ublox Attempt at SEP Fairness

ublox hired me to set up an in-bound licensing program where the modules we sell to our customers would fairly compensate patent holders for the use of the SEPs our modules implement. This basic principle of balancing fairness to our customers and fairness to patent holders is proving to be unrealistic due to an utter lack of transparency and oversight when a small or medium enterprise (SME) like ublox asks for a license from a Non-Participating Enterprise (NPE) or large patent holder that monetizes its SEPs. The current SEP licensing system is defeating for SMEs and, when coupled to actual standards body practices and no-IP license positions by Chinese companies

and others, the system is unbalanced with no level playing field for competing. Manipulation is defeating the FRAND principle and federal court oversight is no solution for many companies[24] and, depending upon a jurisdiction's injunctive practices, may actually exacerbate the SEP/FRAND imbalance.

So, What Should Be Done?

The United States needs to regain leadership in the SEP/FRAND licensing process to make sure SEP holders receive fair compensation for the use of its actual SEPs by all SEP implementers. Currently, both China and the European Union have proposed regulatory oversight to remove the "cloak and veil" from SEP/FRAND licensing, provide guidance, and level the licensing playing field between SEP holders and SEP implementors. This leveling will also benefit module manufacturers in assuring when competing against another module manufacturer, the horizontal competition field is likewise leveled with Chinese module manufacturers paying for SEP use just like a Western module manufacturer.

There are three basic steps that would be a start to leveling both vertical and horizontal competition issues regarding SEPs. A required first step must be **Meaningful Transparency** to identify *actual* SEPs as opposed to making patent implementers rely upon the "believed-SEP" declarations currently

[24] In 2023, ublox filed Federal court litigation against Interdigital, Inc, (IDC) a prominent U.S. SEP holder and ETSI participant. IDC had licensed ublox for over 10 years to its SEPs but then refused to renew the license. IDC had filed hundreds of declarations at ETSI claiming to have cellular SEPs and ublox modules are ETSI standard compliant. The Federal court dismissed the case with IDC stating it neither accused u-blox of infringing its patents nor asked u-blox to take a license, explaining that in earlier negotiations and litigation IDC only asserted infringement in response to ublox's demands for a license. IDC stated, "[it] has no plans to assert its patents against u-blox," regardless of its ETSI SEP licensing commits. (Federal Court, Southern District California, San Diego, Case No. 23CV002 BEN DEB.)

being filed at standards organizations. [25,26] These "believed-SEP" declarations often do not even suggest the section of the standard to which the "believed-SEP" applies. A second basic step would be to define the component or product upon which a royalty may be charged – this is commonly known as the **Royalty Base** – to assure a SEP implementer is not over-charged for SEP usage based upon other technology in the end product and the SEP holder receives a FRAND compensation for actual SEP use.[27] And third, understanding and establishing the **Reasonable Aggregate Value**[28] for a given

[25] I refer to the declarations filed as "believed-SEP" declarations because at the time of filing a declaration at a standards body that references the underlying technical submission made at a work group, it is unknown whether or not the standard will adopt the technical submission as stated by the company or if it will be modified by the work group. Common company practice is to submit a patent application at a patent office concurrent to making the technical submission into the standards work group, meaning the patent application is not connected to the technical submission and may not reflect what actually made it (was accepted) into the standard – analytical data shows most patents generated in this manner are most likely not a SEPs. Yet, patent holders will assert these questionable SEPs during licensing negotiations without ever verifying the actual SEP-ness of the patent to the standard.

[26] Based upon my standards experience since 1995, SEP-declarations required to be filed by standards organizations were never intended to be used in any way for licensing purposes. The intent was to make sure member-companies agreed any patents they held that were SEPs actually included in a standard would be available to proliferate the dispersion of the standard technology and drive technical uniformity to benefit of markets and the general public while driving safe practices. (Example – make sure all 120V electrical plugs in U.S. are three pronged.)

[27] A growing problem in SEP licensing is SEP holders are abandoning their standards licensing commitments in order to boost profits. The easiest way to accomplish this "profit boost" is to refuse to use the royalty base set at the component where the standard technology is actually executed. For example, the wireless module/modem level which, as will be shown by my demonstration, is where the wireless connection to a network occurs. Instead, SEP holders are increasing using the end product as the royalty base, ignoring the fact that the end product tends to include many other technologies and other issues unrelated to the standardized technology.

[28] "Reasonable Aggregate Value" is generically referred to in the industry as Aggregate Royalty Rate or Aggregate FRAND Royalty Rate for the SEP patents used. It is understood that for SEPs, an individual SEP's value cannot be considered in isolation. The parties on

technology used in product verticals wherein the impacts of multiple variables can be weighed and considered. Often forgotten is that the end product user is the one who pays the price for inflated SEP royalties. Non-FRAND royalties paid at any level are passed through to the end user. For SEP-enabled products that support delivery of basic needs such as water, electricity, and transportation, many of the end users are average people who struggle to afford *any* increase in costs.

CONCLUSION

Countering the above competition threats and bringing U.S. leadership in the form of transparency and predictability to the SEP licensing quagmire will empower the domestic IoT industry in the U.S. and Western allies to deliver a secure supply chain which enables growth and innovation. It will greatly empower innovation and SMEs to participate in the markets without fear. The fostering of a strong, globally competitive market for IoT companies will serve to drive industry and innovation in a manner which avoids the risks inherent in any supply chain dominated by CCP controlled companies.

For now, there remains a number of American, European, and Asian players still in the IoT module market, however, this may not be the case for long given the rapid market capture by Chinese module companies.[29] The U.S. and other

---

both sides of the license need to take into account a reasonable aggregate royalty rate for all SEPs in the standard to thereby proliferate the standard's use and discourage proprietary solutions in return for a SEP receiving monopolistic positioning in the final standard. In reality, this requires assessing the value of all SEPs used by the technology. One solution is a neutral entity to determine and make public the total standardized value for SEPs supporting a standardized technology in a market vertical.

[29] It should be pointed out that when the U.S. concerns were raised regarding Huawei and ZTE sales into U.S. markets, the only other supply options were Erikson and Nokia.

nations took action in the areas of 5G and semiconductors when a security threat by Chinese companies was identified and market capture issues arose.[30] This same situation is exactly what is happening now with IoT modules and is gaining speed.

The U.S. urgently needs to act in the field of IoT, to preserve the future of IoT manufacturers based in the U.S. and other countries, and to uphold national security, economic prosperity, privacy and values. The longer the delay in limiting Chinese cellular IoT modules and taking over SEP licensing leadership, the more difficult, expensive, and painful to the markets it will become. The time to act is now.

I thank you again for the opportunity to share these thoughts with you today.

[30] Two smart city deals with local authorities in the United Kingdom were cancelled at the very last minute after intervention by the U.K National Cyber Security Centre and Government Communications Headquarters. (Financial Times). https://www.ft.com/content/46d35d62-0307-41d8-96a8-de9b52bf0ec3 .