23 Jul 2019

It's security, stupid - why it's time to see the wood from the trees in the FTC's case against Qualcomm

In this opinion piece, James Edwards of ELITE Strategic Services, argues that the recent antitrust case won by the FTC against Qualcomm in California is not only legally flawed, but also raises significant security concerns while threatening US technology and IP leadership

The US Federal Trade Commission's (FTC) antitrust lawsuit against chipmaker Qualcomm juxtaposes uncomfortably against the battle between Qualcomm and Huawei for dominance of core 5G technology.

These disputes have profound ramifications for intellectual property rights, Western security and economic competitiveness. Indeed, the security and economic consequences ride on the IP rights.

The outcomes will resonate for a decade or more, until 6G emerges. In fact, the outcomes today for patent licensing and 5G wireless leadership will affect who will be competitive in developing 5G's full possibilities, 6G technology and the future.

Patent licensing at risk

The timing of the FTC lawsuit, aimed at industry-standard patent licensing practice, alongside the 5G leadership contest could hardly be more inopportune. If the district court's broad ruling, which portends to curb licensing dramatically, stands, it will likely clear the field for China's national champions as the global leaders of 5G and beyond.

At the heart of the litigation is the common practice of licensing patent portfolios, as well as requiring a licence in order to obtain microchips. This became the wireless industry practice to achieve greater efficiency for both patent owner and licensee. It is an approach that allows

purchasers to gain access to standard-essential and non-standard-setting patents. Both offerer and purchaser enjoy marked benefits from not having to negotiate licences one patent at a time, when several patents, perhaps some from both categories, are needed.

This discussion isn't intended to debate holdup v holdout or the intricacies of SEPs and FRAND. Suffice it to say that, like Assistant Attorney General for Antitrust Makan Delrahim, my read of the evidence leads me to view the assertions that SEP-owner holdup is a problem with a certain level of scepticism. And I don't believe that innovators relinquish their IP rights when they make FRAND commitments.

Moreover, the dynamic competition sparked by emerging (especially standard-setting) technologies more than offsets short-term cost differences consumers may incur with the breadth of benefits arising from the creation and development of the new market, which patent licensing makes possible. A statement by President Reagan's Commission on Industrial Competitiveness resonates here: "The very act of [patent] licensing is procompetitive rather than anticompetitive."

Regarding the judicial ruling against Qualcomm, in addition to the disruption to industry-standard licensing arrangements, requiring the firm to do business with competitors, out of sync with *Trinko*, and the extraterritorial reach of the injunction are especially disturbing. Also concerning is the fact the standards at issue are at the system level, not the component level. Yet the court ordered component-level licensing.

Ironically, around Apple's and Qualcomm's settlement of their global litigation shortly before the FTC case ruling came down, it emerged that Apple had determined its jilted supplier Intel's chips didn't measure up to the quality of Qualcomm's 5G chips. Apple also decided against developing its own chips, a strategy the company determined would leave it disadvantaged in 5G-capable competition. Intel quickly cut its losses and dropped out of this component space.

The upshot of the court's order, unless stayed and tossed out by the Ninth Circuit, could well be a reduction of Qualcomm's significant budget for research and development — the key to its technological acumen and competitiveness against rival, state-backed Huawei. The line runs from patent licensing to healthy R&D funding to superior, standard-setting engineering. This blow to Qualcomm's virtuous circle carries serious consequences for the economy and security of the United States and its allies.

The public interest

The most important question is what in the public interest is most pressing and most compelling. Is it in an antitrust dispute involving competing corporations over the price of licensing superior innovation (where the FTC has sided with the implementer over the innovator)? Or is the public interest greater in the surrounding national security, economic competitiveness and related intellectual property integrity matters?

In May, the FTC prevailed in federal district court in California scarcely a week after the US Senate Judiciary Committee held a hearing titled "5G: National security concerns, intellectual property issues, and the impact on competition and innovation".

Meanwhile, the litigation puts 5G leadership in question, just as standard-setting is shifting to high

gear and as China redoubles its efforts to win, by hook or by crook, on the standards front.

At the Judiciary Committee, Senator Chris Coons, highlighted the public interest that the federal district court on the other side of the country was simultaneously discounting: "I'm convinced that our ability to be leaders on the global stage depends on our ability to command the intellectual property heights of 5G."

Deputy Assistant Secretary for Cyber and International Communications and Information Policy, Robert Strayer, alerted senators to a critical facet of the public interest - concern for how Western cyber vulnerability in technological systems like 5G exposes free nations and their citizens to more dangerous vulnerabilities. "As the world becomes more interconnected, international cyber policy issues are becoming even more critical to our national security, human rights and economic prosperity," he said.

The State Department witness detailed public interest concerns relating to Huawei's and Qualcomm's contest over core 5G standards: "[W]e are concerned that China could compel actions by network vendors to act against the interests of our citizens or citizens of other countries around the world."

Strayer continued: "Because of the essential role that vendors play in networks and their maintenance, they can be ordered to undermine network security, to steal personal information or intellectual property, conduct espionage, disrupt critical services, or conduct cyber attacks. Under Chinese laws, . . . Chinese citizens and organisations are required to cooperate with Chinese intelligence and security services."

The public interest elements of security, economic competitiveness and IP integrity - dismissed by the FTC and the district court as seen in their aggressive pursuit of SEP patent licensing via the premier US wireless chipmaker - worry the rest of the US government and several Western allies.

For example, federal departments and agencies, including Defense and Energy, urged the FTC to settle with Qualcomm to avoid crippling the technology leader - and thereby the United States. The Justice Department asked the court for a remedies hearing, which the judge denied before issuing a ruling that will certainly advantage China in the 5G race. DOJ has a criminal investigation of Huawei underway related to theft of trade secrets of US businesses, including T-Mobile US's robotics secrets, which the carrier won in civil cases.

A new cybersecurity analysis by Ohio-based Finite State determined that more than half of examined firmware in Huawei telecom network products poses a security risk. Last year, Congress enacted, as part of the National Defense Authorisation Act, a ban on federal agency purchases of Huawei and ZTE equipment, and a block on federal funds going to the same Chinese suppliers.

America and its allies harbour concern about security, economic and other risks if Huawei takes the 5G lead from Qualcomm, because 5G will be a system connecting systems. This exponentially expands the breadth of vulnerabilities of all types.

"When we talk about 5G, we're not talking about hailing a car," Homeland Security's Director of Cybersecurity and Infrastructure Security, Christopher Krebs, told the Senate Judiciary Committee. "We're talking about autonomous vehicles not being able to operate, about telemedicine. This . . .

moves from a data confidentiality issue to a life safety issue, where things won't work as designed, whether . . . the signal's up or down."

Another Senate Judiciary witness, James Lewis of the Center for International and Strategic Studies, warned of China's designs on 5G and beyond: "No one could make 5G without Qualcomm, Cisco, Intel, and other leading US companies. China ... plans ... to end this dependence. It hopes to dominate the telecommunications market using Huawei."

Earlier this year, the UK National Cyber Security Centre reported that Huawei has never fixed software flaws creating security weaknesses in its equipment, first identified years ago. Also, European mobile carrier Vodafone disclosed it had found security weaknesses in 2011 and 2012 in Huawei's products used in Vodafone's Italian network. Australia, Canada, the Czech Republic and other allies have warned of security vulnerabilities in Huawei technology.

"[W]e don't need a smoking gun to know that the risks are intrinsically greater with Chinese equipment, due to the Chinese government's role in ... a state-owned enterprise or state-influenced enterprise," Charles Clancy of Virginia Tech's Hume Center for National Security and Technology said at the Senate hearing. "[I]n many parts of the world, Huawei actually operates the equipment on behalf of host-nation telecommunications companies. A back door is not needed if you already have a key to the front door."

As the Ninth Circuit weighs Qualcomm's appeal, that court should carefully consider the significant public interest in US-based, IP-based competitive leadership in cutting-edge technology, especially a foundational technology such as 5G.

The security implications of not staying and tossing the district court ruling are plain. In 2018, the Committee for Investment in the United States (CFIUS) noted that the "weakening of Qualcomm's position would leave an opening for China to expand its influence on the 5G standard setting process".

CFIUS highlighted Qualcomm's "unmatched expertise". US military and intelligence agencies through CFIUS expressed a high degree of trust and confidence in Qualcomm. Diminished R&D and innovative leadership of Qualcomm would impose "substantial negative national security consequences for the United States". This assessment led the President to block a hostile takeover of Qualcomm, given its crucial role in 5G and the implications of Broadcom's takeover for national and economic security.

The same considerations resound in filings with the Ninth Circuit on Qualcomm's stay motion. The Department of Justice filed a statement of the United States' interest in favour of a stay. Accompanying declarations from the Departments of Defense and of Energy supported DOJ's statement. The FTC's filing doubled down against a stay.

Economically, the stakes are high. If Qualcomm gets a reprieve, 5G will bring the United States a projected $1.3 trillion to $1.9 trillion in economic output by 2035. IHS Markit estimates the 5G value chain will produce $900 billion in output along with 3.6 million jobs. If the FTC wins, the new wealth 5G creates will be largely in China.

It's worth remembering how we got here. And the appellate court would benefit from reviewing a

then-commissioner's dissent when the FTC launched this case. Commissioner Maureen Ohlhausen scathingly called it an "extraordinary situation: an enforcement action based on a flawed legal theory (including a standalone Section 5 count) that lacks economic and evidentiary support, that was brought on the eve of a new Presidential administration, and that, by its mere issuance, will undermine US intellectual property rights in Asia and worldwide."

Should the FTC prevail at the appellate level, the urgent, overarching public interest will have gone unserved, outweighed by myopic, unfounded antitrust concerns. This would likely prove to be a hollow victory for the FTC - at the price of an existential threat from China, which FBI Director Christopher Wray has called a "whole of society threat"

James Edwards is the founder and CEO of ELITE Strategic Services, LLC. He consults on intellectual property and healthcare innovation, as well as regulatory and policy issues.

James Edwards

CEO | ELITE Strategic Services, LLC

TAGS

Patents, **Litigation**, **Law & Policy**, **Frand/SEPS**, **Technology Licensing**, **Valuation**, **Internet**, **Mobile Communications**, **Computers & Software**, **Telecommunications**, **Internet of Things**, **United States of America**, **Asia-Pacific**, **China**, **North America**