Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of Verizon Request for Declaratory Ruling, or, in the Alternative, for Partial Waiver, Regarding the Handset Locking Rule for C Block Licensees	WT Docket No. 06-150

COMMENTS OF DOUBLE PERFECT ON VERIZON'S REQUEST FOR DECLARATORY RULING, OR, IN THE ALTERNATIVE, FOR PARTIAL WAIVER, OF ITS C BLOCK LICENSE OBLIGATIONS

Pursuant to the *Public Notice* released by the Wireless Telecommunications Bureau on March 5, 2019, Double Perfect hereby submits the following comments on the device locking proposal Verizon previewed on September 11, 2018[1] and submitted to the Commission on February 22, 2019.[2]

I. THE FCC SHOULD NOT ISSUE A DECLARATORY RULING OR WAIVE THE C BLOCK LICENSE CONDITIONS.

Limiting the definition of "customer" and/or permitting C Block licensees to lock handsets, temporarily or otherwise, would be inconsistent with the handset locking prohibition[3] and other obligations C Block licensees accepted.[4] Verizon says its device locking proposal will

1 Kellen Barranger, https://www.droid-life.com/2018/09/11/verizons-new-device-unlock-policy-will-lock-phones-for-60-days-or-life-of-payment-plans/ ("Theft is not the only reason for the change, though. Verizon also states that phones purchased on device payment plans could be subject to SIM locks for the entire term of the sales agreement.… To recap, Verizon plans to lock phones for a minimum of 60 days post purchase.")

2 "Verizon" includes Cellco Partnership & Affiliated Entities d/b/a Verizon Wireless.

3 47 CFR §27.16(e) ["*Handset locking prohibited.* No licensee may disable features on handsets it provides to customers, to the extent such features are compliant with the licensee's standards pursuant to paragraph (b) of this section, nor configure handsets it provides to prohibit use of such handsets on other providers' networks."]

4 "C Block" refers to spectrum in the Upper 700 MHz Band C Block.

protect customers and itself from identity theft and fraud,[5] but unfortunately, Verizon's device locking proposal won't protect customers from identity theft and won't prevent fraudsters from using other people's money to buy a $999 phone from Verizon, a $999 phone from an independent retailer that doesn't lock devices, or a $1,999 notebook computer that isn't designed to support allowing an Internet service provider to lock it.

As Verizon notes, sensitive information that makes customers more susceptible to identity fraud is readily available through data brokers and because of data breaches, like those involving Equifax, Marriott, and others.[6] The 2017 data breach at Equifax exposed personal information, including names, birth dates, Social Security numbers, addresses, driver's license numbers, and credit card numbers, for 146 million accounts; the 2018 data breach at Marriott exposed personal information for 500 million guests; and the 2013 data breach at Yahoo! (now owned by Verizon), the largest in history, exposed personal information for three billion accounts.[7] Recently, other data breaches[8] and the sale of customer data from major US cellular carriers through data brokers like LocationSmart and Zumigo[9] have added to the pool of sensitive information available to

5 *Verizon Petition* at 1

6 Declaration of Stephen Schwed at 5 ¶ 11 (February 21, 2019)

7 Soo Youn, *Marriott's data breach is large, but it's not the largest: These are the 5 worst corporate hacks*, https://abcnews.go.com/Technology/marriotts-data-breach-large-largest-worst-corporate-hacks/story?id=59520391 (November 30, 2018) ("That distinction goes to Yahoo — now owned by Verizon — which experienced the largest data breach in history in 2013.")

8 Brian Krebs, https://krebsonsecurity.com/2016/03/crooks-steal-sell-verizon-enterprise-customer-data/ (One or more individuals acquired and sold customer data of 1.5 million Verizon Enterprise customers.) Zack Whittaker, *Millions of Verizon customer records exposed in security lapse*, https://www.zdnet.com/article/millions-verizon-customer-records-israeli-data/ (July 12, 2017) (Customer records for at least 14 million Verizon subscribers, including phone numbers and account PINs, were exposed.)

9 Jennifer Valentino-DeVries, https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html. Zack Whittaker, *US cell carriers are selling access to your real-time phone location data*, https://www.zdnet.com/article/us-cell-carriers-selling-access-to-real-time-location-data/ (May 14, 2018) ('LocationSmart, a California-based technology

identity thieves.

Instead of deferring to Verizon's proposal, the FCC should defer to the FTC. The Federal Trade Commission is the appropriate federal agency to address the root problem recognized by Verizon: identity fraud. The growing prevalence of "SIM swap"-enabled fraud shows that Verizon and other carriers need to invest more to protect customers and avoid becoming enablers of fraud.[10] Fortunately, Verizon and other carriers can choose to become part of a comprehensive solution to the root problem of identity fraud that protects not only Verizon but also customers.

II. By definition, locking handsets configures them to prohibit use on other providers' networks. Thus, permitting C Block licensees to lock handsets, temporarily or otherwise, would be inconsistent with the handset locking prohibition.

By definition, locking handsets, temporarily or otherwise, configures them to prohibit use on other providers' networks. Despite Verizon's claims to the contrary, a 60-day handset lock is a handset lock.

Under Verizon's device locking proposal, legitimate customers will not be able to use their handsets on other providers' networks until after a waiting period (60 days, in Verizon's current proposal) expires. Thus, permitting C Block licensees to lock handsets, temporarily or otherwise, would be inconsistent with the handset locking prohibition.

When the Commission adopted the *700 MHz Second Report and Order*,[11] it did not

---

company, is one of a handful of so-called data aggregators. It claimed to have "direct connections" to cell carrier networks to obtain real-time cell phone location data from nearby cell towers.… Verizon, one of many cell carriers that sells access to its vast amounts of customer location data, counts LocationSmart as a close partner.')

10 Brian Krebs, https://krebsonsecurity.com/2018/11/busting-sim-swappers-and-sim-swap-myths/ ('More importantly, he says, the frequency of SIM swapping attacks is…well, off the hook right now. "It's probably REACT's highest priority at the moment, given that SIM swapping is actively happening to someone probably even as we speak right now," Tarazi said.')

11 *Service Rules for the 698–746, 747–762 and 777–792 MHz Bands et al.*; Second Report and Order; 22 FCC Rcd. 15289 (2007)

equivocate on the handset locking prohibition or other openness rules. The Commission noted Verizon's claims about handset locking and fraud[12] but ultimately found that on balance, bright-line openness rules would provide more investment, innovation, and competition benefits to customers, device manufacturers, application providers, and wireless service providers than equivocal rules, after considering the evidence in the record. For example, the *Report and Order* recognized Columbia Public Law Research Paper No. 07-154,[13] which notes 'Verizon Wireless originally justified crippling Bluetooth on its telephones as a means of preventing "fraud" and virus infections.'[14] After security experts like Jonathan Zdziarski (currently at Apple) scrutinized Verizon's unsubstantiated claims[15] and customers sued, Verizon admitted it crippled Bluetooth to prohibit customers from downloading applications from providers other than Verizon's

12 *Id.* note 430

13 *Id.* notes 457 and 459. Tim Wu, *Wireless Carterfone*. International Journal of Communication, Vol. 1, p. 424, 2007; Columbia Public Law Research Paper No. 07-154. Available at SSRN: https://ssrn.com/abstract=962027.

14 Sascha Segan, *Motorola V710 Review & Rating*, https://www.pcmag.com/article2/0,2817,1639783,00.asp ('But Verizon disabled the phone's Bluetooth file-transfer function, so you can't wirelessly transfer photos to your PC without using the carrier's for-pay Pix Messaging service. Verizon also disabled the built-in Bluetooth Serial Port function, so you have to buy a $39.99 USB cable to sync the phone with your PC. … But even with the USB cable, you can't get photos off the phone or transfer files between the phone and your PC. Verizon says that crippling Bluetooth implementation is a "fraud prevention" tactic to prevent strangers from sending unsolicited text messages to your phone. Whatever.')

15 Jonathan A. Zdziarski, *The Motorola v710: Verizon's New Crippled Phone*, https://web.archive.org/web/20060703041009/http://www.nuclearelephant.com/papers/v710.html ('What Security Issue? I had heard this story from Verizon, which was that they were investigating security issues with the phone, but this appeared only to be an afterthought in comparison with Verizon's profitability needs. The story didn't appear to hold water, and I got the feeling she understood that. Bluetooth has some basic front-line security designed to prevent someone from arbitrarily transferring files to/from the phone without performing a "bonding" ritual. On top of this, the v710 sports a "stealth mode" where it will remain invisible from discovery unless the owner specifically makes it visible (at 60-second intervals) so there's little chance a stranger will even know it's there let alone have the MAC address.")

commercial partners.[16]

III. The Commission should not limit the definition of customer.

The Commission should reject Verizon's call to 'limit the definition of "customer" to someone "responsible for payment" in the context of wireless services and handsets'[17] and declare that the C Block Rules don't apply to customers until after a waiting period (60 days, in Verizon's current proposal) expires. Besides the handset locking prohibition, other parts of the *700 MHz Second Report and Order* and Section 27.16 of the Commission's rules rely on a broader definition of "customer" that recognizes wireless device users are customers of multiple parties, including device manufacturers, application providers, and wireless service providers. Limiting the definition of "customer" would impact not only the handset locking prohibition but also the other customer protections in the C Block Rules. For example, the handset locking prohibition is one half of Rule 27.16(e); the other half prohibits licensees from disabling features on handsets they provide to customers. Clearly, the Commission should not permit licensees to disable features for 60 days (or any other period of time).

Before negotiating a 2012 *Consent Decree* with the Enforcement Bureau,[18] Verizon had compelled application store operators to block tethering applications (to compel customers to pay Verizon additional fees to re-enable built-in tethering features disabled by Verizon). By Verizon's

16 Shelley Solheim, https://www.eweek.com/mobile/verizon-wireless-users-sue-over-disabled-bluetooth-features ("The v710 includes Get It Now, our virtual mall of games and productivity tools that customers can download. The agreements we have with our content providers preclude our allowing anyone to download these applications beyond the phone. The open architecture of Bluetooth could also allow customers to download Get It Now applications beyond the phone," said Verizon Wireless spokesperson Brenda Raney.)

17 *Verizon Request for Declaratory Ruling, or, in the Alternative, for Partial Waiver* at 13 (February 22, 2019) (*Verizon Petition*)

18 *In the Matter of Cellco Partnership d/b/a Verizon Wireless*, File No. EB-11-IH-1311, Acct. No. 201232080028, FRN 0003290673, Order and Consent Decree, 27 FCC Rcd. 8932 (2012) (*Tethering Consent Decree*)

interpretation, wireless device users were customers of application store operators but not Verizon in this instance, and Verizon denied ultimate responsibility for blocking tethering applications from customers:

> A spokeswoman at Verizon suggested that any blocking of the free tethering apps is done by Android OS developer Google. However, she wouldn't say whether Google was doing so at the behest of Verizon or the other carriers.
>
> "Google is ultimately responsible for what is in the marketplace," the Verizon spokeswoman said.[19]

However, the *Tethering Consent Decree* affirmed that in whatever context wireless device users are customers, C Block licensees must not explicitly or implicitly request that applications be made unavailable to them. (Verizon later admitted "one employee" at Verizon was ultimately responsible for blocking tethering applications from customers.[20])

Among other things, the Commission should note that Verizon and AT&T recently colluded to cripple eSIM technology,

> AT&T and Verizon together control about 70 percent of all wireless subscriptions in the United States. A technology that made it easy to switch carriers could lead to more turnover and fewer subscribers for them.…
>
> After the formal complaints against AT&T and Verizon were filed, several device makers and other wireless companies voiced similar concerns to the agency about the carriers' actions around eSIM, four people familiar with the investigation said.
>
> "The actions would limit choice for consumers and harm competition," said Ferras Vinh, a policy expert at the Center for Democracy and Technology.[21]

---

19 Matt Hamblen, https://www.computerworld.com/article/2508454/free-android-tethering-apps-blocked-by-most-carriers.html (May 3, 2011)

20 Brian X. Chen, *F.C.C. Forces Verizon to Allow Android Tethering Apps*, https://bits.blogs.nytimes.com/2012/07/31/fcc-verizon-tethering/ ("The company alluded to the actions of one employee who had been communicating with Google's Android app store operator about the tethering apps.")

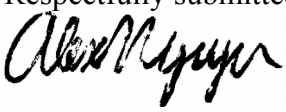
21 Cecilia Kang, *U.S. Investigating AT&T and Verizon Over Wireless Collusion Claim*, https://www.nytimes.com/2018/04/20/technology/att-verizon-investigate-esim.html

And in spite of the C Block Rules, Verizon is currently disabling eSIM technology in devices like Apple iPads and Google Pixel smartphones the carrier provides to customers.[22]

IV. CONCLUSION

The Commission should not issue a declaratory ruling or waive the C Block license conditions.

Respectfully submitted,



Alex Nguyen
Double Perfect
1050 Kiely Blvd. #2608
Santa Clara, CA 95055
408-499-4239
communicator@doubleperfect.com

22 Ina Fried, https://www.recode.net/2016/3/22/11587182/latest-ipad-pro-makes-it-even-easier-to-switch-wireless-carriers ("T-Mobile and Sprint are fully supporting the built-in Apple SIM feature. AT&T, however, will tie the Apple SIM to its network if you buy your iPad at one of its retail stores. Verizon, meanwhile, will require a separate SIM card and disable the built-in embedded Apple SIM on the iPads it sells.") *Disabled eSIM on Pixel 3 devices*, https://www.reddit.com/r/verizon/comments/a73ckj/ ("Verizon has done the same thing to my 2018 iPad Pro. The eSim is disabled and it shipped with a Verizon SIM card in it. There's no way to ever enable the eSim. Verizon sucks.")