No. 2019-1050

UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

VIRNETX INC., LEIDOS, INC., fka Science Applications International Corporation,
Plaintiffs-Appellees,

v.

APPLE INC.,
Defendant-Appellant.

VIRNETX INC.,
Plaintiff-Appellee,

v.

APPLE INC.,
Defendant-Appellant.

On Appeal from the United States District Court for the Eastern District of Texas, Nos. 6:12-cv-00855-RWS and 6:11-cv-00563-RWS, Judge Robert Schroeder, III

NON-CONFIDENTIAL REPLY BRIEF FOR DEFENDANT-APPELLANT APPLE INC.

BRITTANY BLUEITT AMADI
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Avenue NW
Washington, DC 20006
(202) 663-6000

THOMAS G. SPRANKLING
WILMER CUTLER PICKERING
HALE AND DORR LLP
950 Page Mill Road
Palo Alto, CA 94304
(650) 858-6000

WILLIAM F. LEE
MARK C. FLEMING
LAUREN B. FLETCHER
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-5000

Attorneys for Defendant-Appellant Apple Inc.

April 5, 2019

CERTIFICATE OF INTEREST

Counsel for Defendant-Appellant Apple Inc. certifies the following:

1. The full name of every party or *amicus* represented by me is:

Apple Inc.

2. The name of the real party in interest represented by me is:

Not applicable.

3. All parent corporations and any publicly held companies that own 10 percent or more of the stock of the party or amicus curiae represented by me are:

None.

4. The names of all law firms and the partners or associates that appeared for the party or amicus now represented by me in the trial court or agency or are expected to appear in this court (and who have not or will not enter an appearance in this case) are:

WILMER CUTLER PICKERING HALE AND DORR LLP: Dominic E. Massa, Elizabeth Reilly, Rebecca Bact

KIRKLAND & ELLIS, LLP: Robert A. Appleby, Gregory S. Arovas, Akshay S. Deoras, David N. Draper, Jeanne M. Heffernan, Mangesh A. Kulkarni, Joseph A. Loy, Thomas V. Matthew, F. Christopher Mizzo, Steve Papazian, John C. O'Quinn, Aaron D. Resetarits, Leslie M. Schmidt, Diwei Zhang

NELSON BUMGARDNER ALBRITTON PC: Eric M. Albritton, Shawn A. Latchford

DESMARAIS LLP: John M. Desmarais, Edward B. Geist, Ameet A. Modi, Jennifer Przybylski, Michael P. Stadnick, Wesley White

JACKSON WALKER LLP: Brian K. Buss, Christopher N. Cravey, Danny L. Williams

POTTER MINTON, A PROFESSIONAL CORPORATION: John F. Bufe, Michael E. Jones

WILLIAMS MORGAN, PC: Ruben S. Bains, Terry D. Morgan, Matthew R. Rodgers

ALLEN GARDNER LAW, PLLC: Allen Franklin Gardner

AHMAD ZAVITSANOS ANAIPAKOS ALAVI & MENSING PC: Kyung Tai Kim

5. The title and number of any case known to counsel to be pending in this or any other court or agency that will directly affect or be directly affected by this court's decision in the pending appeal:

VirnetX Inc. v. The Mangrove Partners Master Fund, Ltd., Nos. 17-1368, -1383 (Fed. Cir.)

VirnetX Inc. v. Apple Inc., Nos. 17-1591, -1592, -1593 (Fed. Cir.)

VirnetX Inc. v. Black Swamp, IP, LLC, Nos. 17-2593, -2594 (Fed. Cir.)

VirnetX Inc. v. Cisco Systems, Inc., No. 18-1197 (Fed. Cir.)

VirnetX Inc. v. Cisco Systems, Inc., No. 18-1751 (Fed. Cir.)

VirnetX Inc. v. Cisco Systems, Inc., No. 19-1671 (Fed. Cir.)

Inter Partes Reexamination Control No. 95/001,682 (USPTO)

Inter Partes Reexamination Control No. 95/001,714 (USPTO)

Inter Partes Reexamination Control No. 95/001,697 (USPTO)

Dated: April 5, 2019

/s/ William F. Lee

WILLIAM F. LEE
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000

TABLE OF CONTENTS

CONFIDENTIAL MATERIAL OMITTED

The material omitted from page 8 contains confidential technical details concerning Apple's accused products.

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

ARGUMENT

I. THE INFRINGEMENT JUDGMENT FOR THE '135 AND '151 PATENTS SHOULD BE REVERSED.

A. Redesigned VPN On Demand Does Not "Automatically Initiate" A VPN In Response To "Determining" That A DNS Request Is For A Secure Server.

VirnetX concedes that checking ***only*** the requested domain name against the configuration file "determin[es] whether" a secure server was requested. Br. 28 ("Checking against the domain-name list thus serves to 'determine' whether access to a secure site has been requested … as this Court recognized in *VirnetX I*[.]"). VirnetX also acknowledges that redesigned VPN On Demand does not "automatically initiate" a VPN ***in response to that determination***. Instead, as VirnetX admits, VPN initiation depends on another determination performed by the optional probe regarding the requesting device's location. Br. 30 (describing "both the domain-list matching and the firewall probe" and admitting that "[redesigned] VPN on Demand initiates a VPN ***as a result of those checks*** being satisfied").

Thus, as VirnetX's expert conceded—and VirnetX does not deny—redesigned VPN On Demand ***may or may not*** initiate a VPN when "the domain name is on the [configuration file] list" (and therefore the system has determined that a secure server was requested). Apple Br. 34-35 (quoting Appx1448); Appx5055. That cannot satisfy the claims, which require "automatically initiating

the VPN" "***in response to*** determining that the DNS request … is requesting access to a secure target[.]" Appx180(47:20-32); *see* Appx326(48:18-29) ("***when*** the intercepted DNS request corresponds to a secure server, automatically creating a secure channel between the client and the secure server").[1]

VirnetX's arguments are contrary to *VirnetX I* and cannot support the verdict.

First, VirnetX asserts that the optional probe "is ***part*** of determining whether access is being requested to a secure site." Br. 30 (emphasis in original). VirnetX argued the opposite in *VirnetX I*, where it asserted—successfully—that original VPN On Demand "determin[ed] whether" a secure server was requested by simply checking the requested domain name against the configuration file. *VirnetX, Inc. v. Cisco Sys., Inc.*, 767 F.3d 1308, 1320 (Fed. Cir. 2014). The "domain-list matching" accordingly completes the determination whether the request was for a secure server; even if other checks occur, they do not change ***that*** determination.[2]

VirnetX now contends that checking the requested domain name against the configuration file is no longer sufficient to "determin[e] whether" the requested

---

[1] Emphases are added unless indicated otherwise.

[2] VirnetX claims that "domain-list matching [is not] the ***only*** way to satisfy" the "determining whether" limitation. Br. 31 (emphasis in original). But this Court—at VirnetX's urging—rejected the argument that additional steps were needed to determine whether the requested server was "secure." *VirnetX I*, 767 F.3d at 1320.

server is secure. Br. 28-29. Not only is that contrary to *VirnetX I*, but it depends on VirnetX's unsupported and erroneous assertion that whether a ***server*** is secure (*i.e.*, "requires authorization for access," Appx15046) depends on the ***requesting device's*** location. As Apple explained (Br. 37-38), VirnetX's expert never disputed that a server behind a firewall requires authorization for access (and is therefore "secure") even when the requesting device is also behind the firewall—a point that VirnetX leaves conspicuously unrebutted. Thus, the optional probe's check regarding the requesting device's location says nothing about whether the requested server is secure.

VirnetX also invokes (Br. 31) *VirnetX I*'s statement that private networks are "secure and anonymous owing to protection provided by the private network." 767 F.3d at 1321. But that statement nowhere suggests that the security of a server behind a firewall varies depending on the ***requesting device's*** location. As Apple explained (Br. 37-38), a server located behind a private network's firewall "require[s] authorization for access" ***no matter where*** the requesting device is located. Appx2254(204:11-25)(Patience); *see* Appx2346(38:8-23)(Blaze) (device "internal to the company network" still needs "some authorization" to access secure server). Because the patents consider a server "secure" simply because it is listed in a configuration file of "private web addresses"—as the Court held in *VirnetX I*, 767 F.3d at 1320—that same server necessarily remains "secure"

regardless of the requesting device's location. VirnetX's unsupported analogy to a "bank vault" (Br. 31) only reinforces that VirnetX is trying to expand its claims well beyond their terms and construction.[3]

Second, VirnetX contends that redesigned VPN On Demand "***always*** checks the list of secure domains and, when it creates a VPN link, it does so 'in response' to a match." Br. 32 (emphasis in original). But VirnetX then refutes its own argument by conceding that the "addition of the probe means the system might sometimes ***decline*** to create a VPN link ***despite a match***." *Id.*; *see* Br. 14-15. VirnetX further admits that, due to the probe's location check, the same device requesting access to the same secure server will receive a different result—VPN versus no VPN—depending solely on the requesting device's location. Br. 16 (chart showing that "VPN link" to secure server "[f]ound in [l]ist" established only if requesting device is "[o]utside firewall"). In other words, a VPN is not automatically initiated in response to the determination that a secure server is requested (*i.e.*, the domain-list match) as the asserted claims require. The optional probe therefore does not merely "perform[] additional steps" (Br. 32); it takes the accused functionality outside the claims' scope.

---

[3] Contrary to VirnetX's suggestion (Br. 29), Dr. Jones's testimony that the probe's failure indicates that the probe "cannot reach it without authorization" refers to the separate probe server, not the secure server listed in the configuration file. Appx1341; *see* Appx2220-2222; Appx1438-1439.

VirnetX's discussion of the specification (Br. 32-33) adds nothing. As this Court observed, the specification discloses "determin[ing] whether a request is for a secure site by checking the domain name against a table or list of domain names." *VirnetX I*, 767 F.3d at 1320 (citing Appx175(38:23-30)). While it also describes an embodiment including a "check" to "determine whether the user is authorized to connect to the secure host" (Appx176(39:7-9)), "every claim does not need to cover every embodiment." *Pacing Techs., LLC v. Garmin Int'l, Inc.*, 778 F.3d 1021, 1026 (Fed. Cir. 2015). Indeed, unasserted claim 13 of the '135 patent separately recites "authenticating … that the request … is from an authorized client[.]" Appx180(48:29-45); *see PSN Illinois, LLC v. Ivoclar Vivadent, Inc.*, 525 F.3d 1159, 1166 (Fed. Cir. 2008) ("[D]isclosed embodiments may be within the scope of other allowed but unasserted claims.").

Nor do dependent claims 4 and 5 compel a different conclusion. Each recites a step in which, if the requesting "client computer" is not properly "authorized," the system "return[s] an error from the DNS request." Appx180(47:41-52). That additional step does not—and cannot—eliminate claim 1's requirement that a VPN is "automatically initiat[ed]" "***in response to*** determining" that a secure server is requested. Appx180(47:29-32). To the extent VirnetX suggests otherwise, the dependent claims would be invalid. *Multilayer Stretch Cling Film Holdings, Inc. v. Berry Plastics Corp.*, 831 F.3d 1350, 1362

(Fed. Cir. 2016) ("A dependent claim that contradicts, rather than narrows, the claim from which it depends is invalid.").

VirnetX's contention that the optional probe "governs later DNS queries" (Br. 33) is incorrect and irrelevant. As Apple explained (Br. 36-37), redesigned VPN On Demand consults the result of the probe's location check ***after*** checking the requested domain name against the configuration file. Appx2256-2258 (explaining logical flow of decisions); Appx5055 (depicting "Optional HTTPs Probe" after "VPN Config Matching"). Only ***after*** the results of the probe are consulted—and only if it determines that the requesting device is outside the firewall—does redesigned VPN On Demand initiate a VPN. Appx5055; Appx2258(Patience).[4]

Third, VirnetX attempts (Br. 33-34) to brush aside its prior concession regarding original VPN On Demand's non-infringing "If Needed" mode. VirnetX improperly relies upon expert testimony from the ***2012 trial***, which cannot support

---

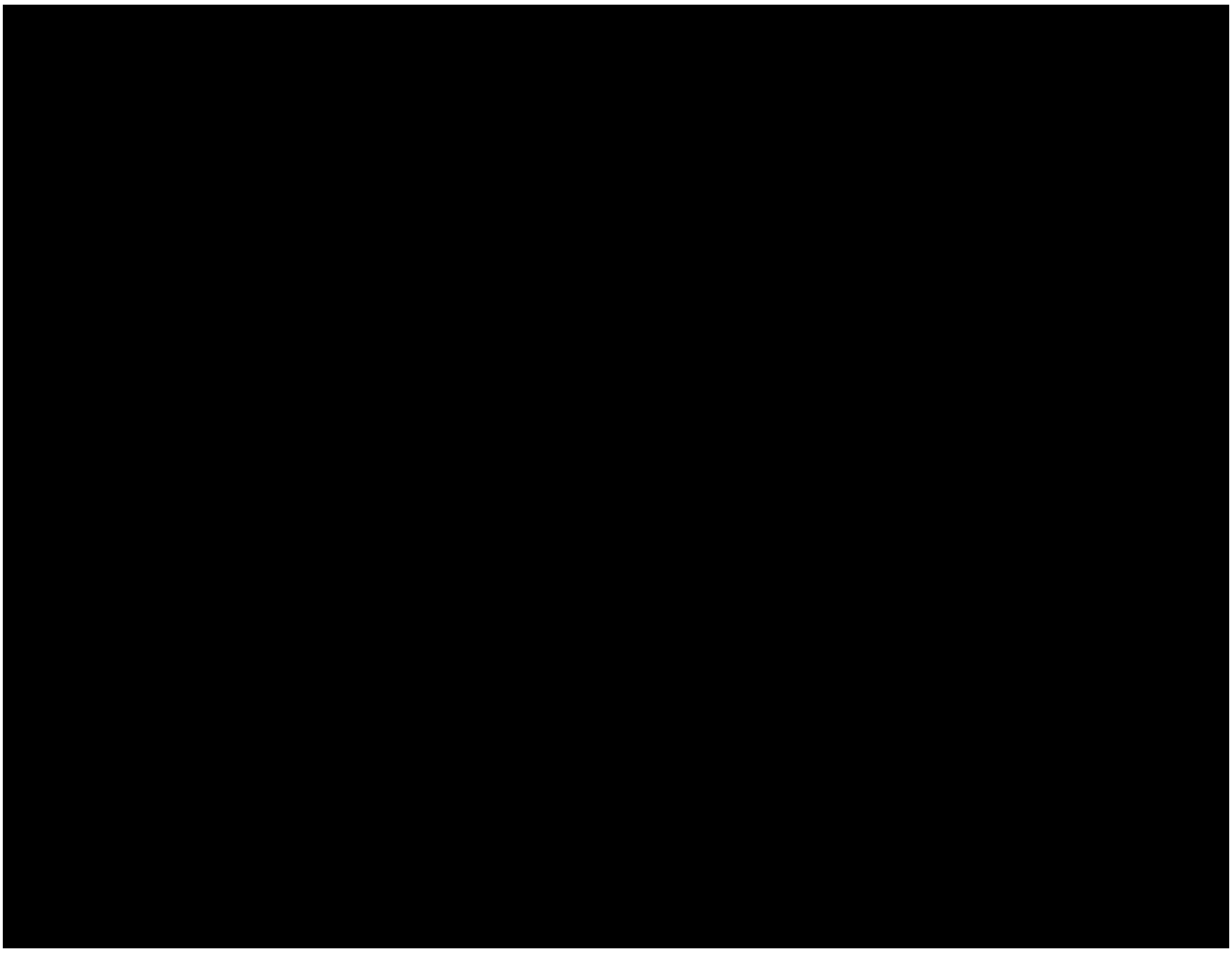
[4] VirnetX does not dispute this order of operations. Instead, it vaguely says the probe "is not deployed ***after*** domain-list matching." Br. 33 (emphasis in original). But the relevant event is when the results of the probe's location check are used, not when the probe is "deployed."

VirnetX also asserts that Apple's expert "conceded that, whenever the user is outside the firewall, VPN on Demand consults 'whether the [requested] domain name matches' the configured list of domains and thereby decides whether a VPN link is created." Br. 17 (partially quoting Appx2393) (emphasis omitted). Dr. Blaze said no such thing. Rather, he explained that the "outcome depends on whether you're in a ***location*** where the probe succeeds or fails." Appx2393(85:18-24).

the ***2018 verdict***. Appx27797. Even so, Dr. Jones did not describe the original "If Needed" mode as "a conventional DNS query" as VirnetX contends; he described it as the "antithesis of the [A]lways" mode that was found to infringe. *Id.*

At the trial in this case, Apple engineer Simon Patience testified—without contradiction—that the original "If Needed" mode checked whether the server name is "on the list" ***and*** "whether [the] device is inside or outside the firewall." Appx2204-2208; *see* Appx10063 ("If Needed" mode of "VPN On Demand does not always initiate a VPN connection"). It then initiated a VPN only after determining that the requesting device was outside the firewall—***even if*** the requested domain name was in the configuration file. Appx2201; Appx2205-2208. Redesigned VPN On Demand does the same thing.

VirnetX now claims that the original "If Needed" mode "did not infringe because it tried to create an unsecured link to any server found in a conventional DNS." Br. 34 (emphasis omitted). The same is true of the implementation VirnetX accuses here. As shown in the flowchart below (misleadingly truncated by VirnetX, Br. 29), redesigned VPN On Demand first checks whether the requested domain name matches the configuration file ("VPN Config Matching"). If so, it attempts to create an unsecure connection by sending a conventional DNS request ("DNS Query"), shown in the red box:



Appx5055 (annotation added; excerpted). VirnetX identifies no meaningful distinction between the original "If Needed" mode—which it conceded did not infringe (Apple Br. 10)—and the accused implementation of redesigned VPN On Demand.

B. VirnetX's Assertions Of Direct And Induced Infringement Fail.

VirnetX does not deny that redesigned VPN On Demand can be used in non-infringing ways; it accuses only a narrow, optional implementation that is disabled by default. Apple Br. 40. VirnetX nonetheless argues that ***every***

customer who bought an accused Apple device practiced the asserted claims in the United States at Apple's inducement. Its arguments fail.

'135 Patent. VirnetX does not deny its obligation to prove that "the steps of the method were actually performed … in the United States." *E-Pass Techs., Inc. v. 3Com Corp.*, 473 F.3d 1213, 1222 (Fed. Cir. 2007). VirnetX's primary assertion is that a user "***can*** 'replicate' the infringing 'Always' mode" (Br. 36)—namely by misconfiguring the probe to always fail, something VirnetX did not prove Apple ever suggested or anyone ever did (Apple Br. 42 & n.6; Appx1519(66:3-11)).[5] VirnetX does not address, let alone distinguish, this Court's rulings that the mere fact that accused products "could infringe" does not permit finding induced infringement. *E.g.*, *Mirror Worlds, LLC v. Apple Inc.*, 692 F.3d 1351, 1361 (Fed. Cir. 2012) ("Evidence of actual use of each limitation is required."). VirnetX's excursion into the development history of VPN On Demand (Br. 34-38) does not satisfy its burden to "point to specific instances of direct infringement." *ACCO Brands, Inc. v. ABA Locks Mfr. Co.*, 501 F.3d 1307, 1313 (Fed. Cir. 2007). "'[I]f it was inconceivable to [VirnetX] that the accused feature[] w[as] not practiced, … it should have no difficulty in meeting its burden of proof and introducing

[5] Apple's engineer did not testify that "when a device is outside the firewall, 'Evaluate Connection' mode 'replicate[s]' old VPN on Demand's 'Always' mode." Br. 17 (citing Appx1387-1388). He merely recognized "it was ***possible*** to replicate the Always feature," not that every use of "Evaluate Connection" did so. Appx1387-1388.

testimony.'" *Mirror Worlds*, 692 F.3d at 1362; *see also E-Pass*, 473 F.3d at 1222-1223.

VirnetX separately did not show that Apple ***induced*** any customer's direct infringement. VirnetX notably abandons the district court's speculation that a draft test plan that "[i]deally" "would be presented" to an unidentified customer somehow proved that the claimed steps were performed in the United States. Apple Br. 43. VirnetX instead argues that inducement could be inferred from Apple's mere "design[]" of an application with one accused use and other non-infringing uses (Br. 38), but that is contrary to law. *Mirror Worlds*, 692 F.3d at 1361-1362 (design of accused features "cannot serve as the basis for induced infringement" where the claims "require additional user action beyond just turning on the tools").[6]

VirnetX's assertion that Apple "instructed users to configure VPN on Demand in the infringing mode" (Br. 38) is likewise unsupported. VirnetX cites only a "Developer" document identifying the probe as "*Optional*." Appx10079; Appx10121. VirnetX offered no evidence as to the "dissemination" of the

[6] *Water Technologies Corp. v. Calco, Ltd.*, 850 F.2d 660, 668 (Fed. Cir. 1988), did not involve a product with non-infringing uses; the defendant helped the direct infringer "make the infringing resins." VirnetX cites no case suggesting that "designing" a product with non-infringing uses permits finding inducement. *See Dynacore Holdings Corp. v. U.S. Philips Corp.*, 363 F.3d 1263, 1277 (Fed. Cir. 2004) (sale of products "capable of substantial non-infringing uses" is not inducement).

"Developer" document, much less that every Apple customer received it. *Lucent Techs., Inc. v. Gateway, Inc.*, 580 F.3d 1301, 1318 (Fed. Cir. 2009); *see ACCO*, 501 F.3d at 1313 (no inducement where evidence did not show that purchasers received "hang card" instructing performance of claimed method). VirnetX did not even try to prove that someone who read the "Developer" document was moved to practice the accused optional implementation. *Dynacore*, 363 F.3d at 1274 ("To prevail [on] indirect infringement, Dynacore must first prove that the defendants' actions ***led to*** direct infringement."); *Crystal Semiconductor Corp. v. TriTech Microelectronics Int'l, Inc.*, 246 F.3d 1336, 1351 (Fed. Cir. 2001) ("Inducement only occurs if the party being induced directly infringes the patent.").

Even if VirnetX had shown that "some subset" of Apple's customers used the optional probe in the United States—which was all the district court said (Appx87)—VirnetX still failed to limit its damages demand to "the extent to which the infringing method has been used." *Lucent*, 580 F.3d at 1335; *see also Dynacore*, 363 F.3d at 1274 ("Plaintiffs who identify ***individual*** acts of direct infringement must restrict their theories of vicarious liability—and tie their claims for damages or injunctive relief—to ***the identified act***." (emphases in original)). Feedback from one Australian commentator (Appx10066-10068) and one company, Eli Lilly (Appx1388-1389, Appx10070)—not multiple "companies"

(VirnetX Br. 41)—cannot support a damages award for every Apple product sold with redesigned VPN On Demand in the United States.

Contrary to VirnetX's assertion (Br. 40-41), this is not a *Daubert* argument, but a JMOL argument: because ***no*** evidence suggests that all Apple customers were induced to use the accused implementation, no reasonable jury could have awarded damages based on every accused product. Apple did not need a *Daubert* motion or expert testimony to point out VirnetX's failure of proof.[7]

VirnetX's cursory argument that Apple directly infringed fares no better. VirnetX ventures that "(California-based) engineers" might have tested the accused implementation (Br. 37), but neither it nor the district court made such an argument below or pointed to such evidence. Dr. Jones (Appx1386) referred only to a "draft" test plan that, as Apple explained and VirnetX does not deny, was seven steps removed from VirnetX's infringement theory. Apple Br. 41. And VirnetX provided no valuation of the mere ability to "test" an optional feature for which no actual U.S. usage was proven. *Lucent*, 580 F.3d at 1334 ("The damages award ought to be correlated, in some respect, to the extent the infringing method is used

[7] Contrary to VirnetX's waiver argument (Br. 40-41), Apple preserved the point at JMOL (Appx16367, Appx16405); VirnetX did not argue waiver below (Appx16466); and the district court addressed Apple's argument on the merits, albeit incorrectly conflating it with liability (Appx94).

by consumers. This is so because this is what the parties to the hypothetical negotiation would have considered.").

'151 Patent. VirnetX argues that "a need for configuration does not overcome infringement." Br. 39. But as even VirnetX's cited case confirms, that is at most true when the claim "recites capability and not actual operation." *Finjan, Inc. v. Secure Computing Corp.*, 626 F.3d 1197, 1204 (Fed. Cir. 2010) ("the 'reasonably capable' test applies '***only*** to claim language that specifies that the claim is drawn to capability'"); *see* Apple Br. 44-45. VirnetX points to no "capability" language in claim 13; on the contrary, it claims "instructions that, ***when executed, cause*** a data processing device to perform" the claimed steps. Appx326(48:19-21). That claims "actual operation," not capability. And VirnetX has no response to Apple's alternative point that even capability claims are infringed only if "the unmodified accused devices" are reasonably capable of performing the claimed functions. Apple Br. 45. Contrary to VirnetX's suggestion (Br. 40), enabling the optional probe requires more than "setting up a configuration file"; a new server must be installed and the software altered by an IT professional before the probe can be used. Appx2218-2220.

II. THE INFRINGEMENT JUDGMENT FOR THE '504 AND '211 PATENTS SHOULD BE REVERSED.

A. The District Court Erroneously Instructed The Jury That The Claimed "DNS System" Does Not Incorporate The "DNS" Construction.

VirnetX does not dispute that redesigned FaceTime fails to return an IP address and therefore avoids infringement under the district court's "DNS" construction. Instead, VirnetX argues that the claimed "DNS system" does not require a "DNS." That makes no sense. The term "DNS" must have the same meaning everywhere it appears in the claims, not just where convenient for VirnetX. That is how the parties litigated the 417 Action, and Apple timely raised this issue when VirnetX changed its position in this 855 Action. The district court's erroneous pre-trial ruling (Appx19, Appx26684) and subsequent jury instruction (Appx2758) require reversal or at least a new trial.

1. The claimed "DNS system" must include a "DNS."

The claimed "DNS system" expressly requires a "DNS" as a matter of plain meaning. VirnetX does not deny that it agreed to this point in the 417 Action. Apple Br. 47-48; Appx20024. Nor does VirnetX challenge the construction that a "DNS" is "a lookup service that returns an IP address for a requested domain name to the requester." Appx22214; *see* Appx15064.

VirnetX instead points to ***additional*** limitations on the "DNS system," such as the requirement of providing an indication that the system supports establishing

a secure communication link. Br. 45. But those other requirements explain how the claimed "DNS system" must be configured. Appx262(55:49-56) (reciting "a [DNS] system configured to …"). They do not—and cannot—remove "DNS" from the claimed "DNS system."

VirnetX's attempt (Br. 46) to broaden the asserted claims based on the specification fares no better, and was rejected by the district court (Judge Davis) in construing "DNS." Like the claims, the specification describes the invention as including a DNS. *E.g.*, Appx192 (describing invention as "[a] secure [DNS] for a computer network"); Appx238(7:27-29) ("The present invention provides a [DNS] that provides secure computer network addresses for secure … domain names."); Appx254(49:1-2) (describing invention as "[s]ecure [DNS]"). While the specification describes providing a "secure" DNS, it explains that the system is "built on top of the existing Internet protocol (IP)." Appx237(6:21-24). And—like any DNS—the "secure [DNS]" still "provid[es] a way to register and serve domain names and addresses." Appx237(6:32-35); *see* Appx192(abstract); Appx238(7:27-29); Appx260(51:11-12). Thus, as Judge Davis explained with reference to the specification, the "modified DNS server … return[s] an address to the requesting client computer." Appx22214; *see* Appx253(38:36-42).

VirnetX's claim-differentiation argument (Br. 46-47) cannot take the "DNS" out of "DNS system" either. Dependent claims 14 and 15 provide further

limitations describing how the claimed "DNS system" must be "configured." Appx262(56:27-34) ("to respond to the query for the network address"; "to provide, in response to the query, the network address corresponding to a domain name from the plurality of domain names and the corresponding network addresses"). Dependent claim 35 adds that the "DNS system" must contain a "domain name database." Appx263(57:39-47). These ***additional*** limitations are consistent with claim 1's requirement of a "DNS system." They do not—and cannot—expand the claimed "DNS system" to cover systems without a DNS. *Curtiss-Wright Flow Control Corp. v. Velan, Inc.*, 438 F.3d 1374, 1381 (Fed. Cir. 2006) ("[C]laim differentiation 'can not broaden claims beyond their correct scope.'").

2. Apple preserved its argument.

Apple preserved its argument that the claimed "DNS system" includes a "DNS." The district court did not find waiver. *See* Appx19. And VirnetX does not deny that Apple timely requested a construction of "DNS" that includes the "return-of-an-IP-address" limitation. Appx21108; Appx26172. Judge Davis adopted Apple's proposed "DNS" construction in the 417 Action, and confirmed that it continued to apply in the 855 Action. Appx22214; Appx15064.

VirnetX's waiver argument (Br. 42-43) is instead premised on its assertion that Apple was somehow required to request a separate construction expressly

saying that the claimed "DNS system" requires a "DNS." That is incorrect. Both parties ***agreed*** that the term "DNS system" incorporates a "DNS." Apple Br. 47-48 (citing claim-construction briefing and charts). Moreover, as VirnetX conceded below (Appx20024) and seemingly acknowledges now (Br. 47), the plain meaning of "DNS system" includes a "DNS." The words are already there. There was accordingly no reason—much less an obligation—for Apple to repeat the same "return-of-an-IP-address" limitation for the term "DNS system." That is especially true given that, as VirnetX does not deny, the parties and their experts treated the claimed "DNS system" as including a "DNS" during ***years*** of litigation regarding original FaceTime. Apple Br. 47-49.

VirnetX's statement (Br. 42-43) that the district court's *Markman* order "did not address the term" is misleading at best. The district court (Judge Davis) adopted its prior construction of "DNS," which included the "return-of-an-IP-address" limitation. Appx15064. The court had no reason to repeat that limitation for "DNS system."

VirnetX's suggestion (Br. 43) that Apple "disclaimed seeking a claim construction" is also inaccurate. Apple moved to exclude Dr. Jones's non-infringement opinion because he did not (and could not) opine that redesigned FaceTime satisfied the "return-of-an-IP-address" requirement. Appx15149. Apple's motion did not seek "to revisit any claim construction" rulings (VirnetX

Br. 43) precisely because Apple understood—based on the plain claim language, the district court's constructions, and the litigation history—that the claimed "DNS system" included a "DNS." Appx15591. Shortly before trial on redesigned FaceTime, the court (Judge Schroeder) reached a different conclusion, holding that "DNS" and "DNS system" are "separate terms with different constructions," but that was done over Apple's objection. Appx19; Appx26684; *see* Appx15577-15592.

VirnetX's assertion (Br. 43) that Apple conceded it "***never***" argued that "DNS system" incorporates the "DNS" construction or relied on the term "DNS system" for non-infringement is flat wrong. As Apple explained (Br. 22, 47-50), Apple made exactly those arguments before trial and preserved them. VirnetX misleadingly quotes Apple's counsel's confirmation that Apple did not argue non-infringement based on "DNS system" ***to the jury***—because Judge Schroeder's pre-trial ruling foreclosed such an argument. Appx2639.

VirnetX's contention (Br. 43-44) that Apple did not raise its claim-construction argument "until its post-trial motions" is likewise untrue. Apple timely made the argument ***twice before trial***: in its motion to exclude Dr. Jones's non-infringement opinion, and in response to VirnetX's "emergency" motion to clarify the meaning of "DNS system." Appx15539-15540 & n.1; Appx15147-15149 & n.2; Appx15577-15592. After Apple repeated its objection post-trial, the

district court "decline[d] to reconsider its previous rulings" (Appx76-77)—thus making clear that Apple ***had*** raised the argument before—and never suggested that Apple insufficiently preserved it.

Finally, VirnetX points to the district court's ruling in the 417 Action that the term "DNS system" "does not require construction." Appx22219. But as Apple explained (Br. 48) and VirnetX does not deny, that order decided whether the claimed "DNS system" ***additionally*** required being "capable of differentiating between … standard and secure top-level domain names." Judge Davis's *Markman* order never suggested that the claimed "DNS system" did not include a "DNS." *See* Appx22219. Nor would such a ruling have made sense, as both parties agreed that it did. Appx20024; Appx21303-21304. In any event, by concluding that no construction was necessary, Judge Davis gave "DNS system" its plain meaning—which includes a "DNS."

3. The "DNS" instruction was prejudicial.

Even if the instruction had correctly interpreted "DNS system," it was still unfairly prejudicial to give it. VirnetX oddly suggests (Br. 47-48) that the instruction was needed to prevent the jury from applying the "ordinary and accustomed meaning" of "DNS system." Appx2758. Of course, that only reinforces that the claimed "DNS system" includes a "DNS," and that the district court's contrary ruling and instruction were legally erroneous.

VirnetX also claims (Br. 48) that a single statement from Apple's expert at trial warranted the instruction. VirnetX fails to mention (but does not deny) that ***VirnetX's counsel***—not Apple's counsel, as the district court erroneously stated (Appx98-99)—elicited that statement from Dr. Blaze (which he promptly clarified). Appx2412-2413; Appx2421-2422. A party cannot leverage its own invited testimony to justify a prejudicial instruction. *See United States v. Baytank (Houston), Inc.*, 934 F.2d 599, 606 (5th Cir. 1991).

Moreover, the extraneous instruction unfairly suggested that the failure to return an IP address could not be a basis for non-infringement (which was important to Apple's "indication" defense). Apple Br. 51. VirnetX's only response, that the instruction "did not mention IP addresses" (Br. 48), ignores that the "DNS" construction with the "IP address" language was discussed at trial and "provided in [the] juror notebook." Appx2758; *see* Appx1339; Appx16488.

B. Redesigned FaceTime Does Not Provide The Claimed "Indication."

According to VirnetX, redesigned FaceTime infringes because it "***supports*** establishing a direct link." Br. 52. But the asserted claims require more—namely, "an ***indication*** that the [DNS] system supports establishing" a communication link that is direct, secure, and anonymous. Appx262(55:54-56); Appx402(57:43-46); *see VirnetX I*, 767 F.3d at 1317-1319 ("secure communication link" means "a direct communication link that provides data security and anonymity").

The undisputed facts demonstrate that the Accept Push message in redesigned FaceTime does not "indicate" support for a ***direct*** communication link. VirnetX concedes that two devices "need each other's IP address" for direct communication and that "[t]he Accept Push does not include the callee's actual IP address[.]" Br. 50-51, 19. VirnetX thus acknowledges that a "caller can't initiate a direct FaceTime call … based on the contents of the [A]ccept [Push] message alone." Br. 51 (alterations in original). Instead, as VirnetX concedes, the two devices must "exchange ***additional data*** with each other" to "initiate [a] 'direct' … call." Br. 49 (quoting Appx1362-1364).

In short, VirnetX identifies nothing in the Accept Push message that indicates that the system supports a direct communication link. Its efforts to backfill this gaping hole fail.

First, VirnetX asserts that the Accept Push message "contains information the caller needs to initiate the direct link," pointing to the "certificate," "push token," and "certificate name." Br. 49. But as Dr. Blaze explained, none of those items "indicates" that the system supports establishing a ***direct*** link. Appx2321-2323; Appx2328-2330. Rather, "[e]very one of those things is useful for … relayed or ***indirect***" communication. Appx2329.[8]

[8] In passing, VirnetX mentions "several items" in the Accept Push message that refer to "peer" calls. Br. 53. Dr. Jones offered no testimony that those items

Critically, Dr. Jones offered no contrary testimony. *See* Appx1376-1378. Instead, he merely testified that the Accept Push message is "an indication that the provisioning process has been completed." Appx1378. But completion of the "provisioning process" at best indicates support for communication generally; it does not indicate support for ***direct*** communication specifically. Appx2328-2329.

Second, VirnetX asserts that the Accept Push message provides the claimed "indication" using "means other than returning the callee's IP address." Br. 50 (emphasis omitted). But VirnetX still identifies nothing in the Accept Push message that indicates support for direct communication as opposed to indirect communication. It points to nothing, because—as Dr. Blaze testified without contradiction—"[t]here's nothing in the [A]ccept [Push] message to indicate that." Appx2323. That testimony is fully consistent with the district court's construction, which explained that the claimed "indication" cannot be "'the ***mere*** return of requested DNS records, such as an IP address or key certificate.'" Appx15051. However, something—whether that includes an IP address or is something else entirely—must still "indicat[e]" support for a communication link that is ***direct*** (as well as secure and anonymous). *Id.*; *VirnetX I*, 767 F.3d at 1317-1319; *see, e.g.*, Appx260(51:64-67) (describing embodiment using "icon" to indicate that system

---

indicate support for a direct link. *See* Appx1377. Dr. Blaze's unrebutted testimony was that they do not. Appx2328-2329.

supports "secure communication link"). With the removal of the callee's IP address in redesigned FaceTime, there is nothing left in the Accept Push message to indicate such support.

VirnetX attempts to brush aside Apple's redesign by arguing that "direct FaceTime calls happen despite the callee's IP address being absent from the Accept Push." Br. 50-51. That is true, but irrelevant. The claims do not merely recite a system in which direct calls "happen." They require an "indication" of support for a direct communication link, and nothing in the Accept Push message—the ***only*** thing VirnetX identified as the claimed "indication" (Appx1376; Appx1501; Appx2710)—does that. *See supra* pp. 21-22. That the separate "Initiate Push" message contains the caller's IP address, which the callee's device may later use to transmit data packets to the caller (through the "ICE protocol"), cannot change that fact. *See* VirnetX Br. 19-20, 51.[9]

Similarly, the "callee's certificate" in the Accept Push message (VirnetX Br. 51) undisputedly contains no information to indicate that FaceTime supports establishing a "direct" communication link. As both experts explained, the callee's certificate is merely "the beginning of the exchange to create the key that's going

[9] Neither Apple nor Dr. Blaze contended that the indication must "include ***every*** piece of information used to establish the link." VirnetX Br. 52 (emphasis in original). Apple's position has been—and remains—that the "indication" must have something that indicates support for a direct link.

to be used for encryption of that audio/video communication." Appx1482(Jones); *see* Appx1503, Appx1526(Jones); Appx2329-2330(Blaze). In other words, the callee's certificate confirms that a message's ***content*** is secure—*i.e.*, data security, *see VirnetX I*, 767 F.3d at 1317-1318—but it does not indicate whether the communication is ***direct***. Appx2430(Blaze) ("What the certificate is telling you is the key material that you'll use to encrypt messages for that device. And that has nothing to do with direct or indirect[.]"). Dr. Jones never explained how that certificate supposedly indicates support for a ***direct*** link. *See* Appx1376. Rather, he admitted that "***both*** indirect calls on relay and direct calls will require a certificate." Appx1504; *see also* Appx1526-1527(Jones); Appx2328-2329(Blaze).[10]

Third, VirnetX attempts to distinguish the undisputedly non-infringing April 2013 version of FaceTime because "[t]he version accused here supports establishing a direct link—and so infringes." Br. 52. But again, the claims do not cover merely "support[ing] establish[ment]" of a direct communication link; the system must ***indicate*** that it does so. After Apple removed the callee's IP address from the Accept Push message in the April 2013 version and in the accused

[10] The fact that original FaceTime could also ***establish*** both indirect and direct communications (VirnetX Br. 53) is irrelevant. In original FaceTime, the Accept Push message included something (the callee's IP address) ***indicating*** support for direct calls. Appx2113; Appx2297-2298. That was removed from redesigned FaceTime.

version, there was nothing left in the Accept Push message that provided the claimed "indication." Apple Br. 17, 52-53.

III. THE DISTRICT COURT ERRED BY APPLYING ISSUE PRECLUSION TO ALL OF APPLE'S INVALIDITY DEFENSES AND COUNTERCLAIMS.

As Apple explained (Br. 55-58), the district court erred by holding that a prior no-anticipation ruling in the 417 Action barred Apple's obviousness and non-joinder defenses in this 855 Action through issue preclusion. *Voter Verified, Inc. v. Election Sys. & Software LLC*, 887 F.3d 1376 (Fed. Cir. 2018) (issue preclusion did not bar defendant who lost invalidity challenges under §§ 102 and 103 from pursuing § 101 challenge in second case). VirnetX's three responses lack merit.

First, VirnetX asserts that all invalidity defenses are ***always*** a single issue for preclusion purposes. Br. 53-55. But this Court has never so held. VirnetX cites only district court decisions—most predate *Voter Verified*, and the other recognized that *Voter Verified* "casts some doubt on" such decisions. *XpertUniverse, Inc. v. Cisco Sys., Inc.*, 2018 WL 2585436, at *4 (N.D. Cal. May 8, 2018).[11]

[11] *Dana v. E.S. Originals, Inc.*, 342 F.3d 1320, 1325 (Fed. Cir. 2003), held that a party could not raise "the same argument" regarding "the same patent [and] the same accused products" in a later proceeding by presenting "different evidence, including a new expert witness declaration." By contrast, Apple sought to litigate new ***issues***, including obviousness and non-joinder.

VirnetX's attempts to distinguish *Voter Verified* fall flat. This Court ***did*** consider—and expressly stated—that "the § 101 issue was not actually litigated" because it "was in fact barely considered." 887 F.3d at 1383. If all invalidity defenses were the same "issue" for preclusion purposes, the Court would have had to consider whether the prior determination that claims "were not invalid under §§ 102 and 103" (*id.*) meant that "invalidity" (including § 101) had been "actually litigated." Instead, the Court considered the § 101 issue standing alone, indicating that § 101 was a separate issue from the previously-litigated §§ 102 and 103 issues.[12]

VirnetX also argues that the *Voter Verified* defendants did not actually litigate ***any*** invalidity issue. Br. 56. Again, VirnetX is flat wrong. Earlier opinions in the case show that the defendants "sought declaratory judgments of invalidity on various grounds including anticipation, obviousness, and indefiniteness." *Voter Verified, Inc. v. Premier Election Sols., Inc.*, 698 F.3d 1374, 1379 (Fed. Cir. 2012); *see Voter Verified, Inc. v. Premier Election Sols., Inc.*, 739 F. Supp. 2d 1340, 1351-1355, 1363 (M.D. Fla. 2010) (considering various challenges under §§ 102, 103, and 112).

[12] Invalidity defenses under different statutory sections are not merely different "theories." *See* VirnetX Br. 54 (emphasis omitted). Each statutory section presents a different "issue" (*e.g.*, anticipation); a defendant may then present different "theories" (*e.g.*, express vs. inherent anticipation) to prove that defense.

VirnetX takes language from the earlier *Voter Verified* ruling out of context. Br. 56. This Court quoted a district court ruling describing a particular supplemental brief tasked with "addressing the issue of invalidity under 35 U.S.C. § 103"; that brief addressed obviousness for one claim but not others, and thus "fail[ed] to present any argument or evidence regarding the invalidity ***of th[o]se claims***." *Voter Verified, Inc. v. Premier Election Sols., Inc.*, 2011 WL 233804, at *11 (M.D. Fla. Jan. 24, 2011). The same order states that the defendants had viable arguments under §§ 102, 103 and 112 on several claims. *Id.* at *11 n.10.

Second, VirnetX claims there is no "principled basis" for treating anticipation and obviousness as different issues for preclusion purposes. Br. 56-58. But this Court has long held that anticipation under § 102 and obviousness under § 103 are distinct issues—they are "separate conditions of patentability ***and therefore separate defenses***." *Cohesive Techs., Inc. v. Waters Corp.*, 543 F.3d 1351, 1363-1364 (Fed. Cir. 2008); *see Minkin v. Gibbons, P.C.*, 680 F.3d 1341, 1351 (Fed. Cir. 2012) ("[A]nticipation and obviousness are separate conditions of patentability, requiring different tests and different elements of proof."). Thus, "[o]bviousness can be proven by combining existing prior art references, while anticipation requires all [claim] elements … disclosed within a single reference." *Cohesive*, 543 F.3d at 1364. And, unlike anticipation, "obviousness requires analysis of secondary considerations of nonobviousness[.]" *Id.*

To be sure, the Court has generally stated that "anticipation is the epitome of obviousness." *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548 (Fed. Cir. 1983). But more recent precedent "has rejected reliance on th[at] 'legal homily,'" recognizing that claims may be anticipated yet not obvious. *Cohesive*, 543 F.3d at 1364 n.2 (describing nonobvious metal alloy that was anticipated by alchemy textbook).

This principle—that the various statutory invalidity defenses are legally distinct—applies beyond anticipation and obviousness. *Orexo AB v. Actavis Elizabeth LLC*, 2019 WL 1177715, at *8 (D. Del. Mar. 12, 2019) ("validity should not, as a matter of law, be treated as a single issue for estoppel purposes," because there is "no uniformity among the rules that govern the invalidity defenses"). VirnetX does not even attempt to explain why a finding that a claim recites patentable subject matter, for example, bars a later argument that the claim is not enabled.[13]

VirnetX argues that a party cannot argue obviousness based on a reference previously found not to anticipate. Br. 57-58. That is a strawman. Apple's

[13] VirnetX argues that non-joinder and anticipation both fall under pre-AIA § 102. Br. 58. But non-joinder can also depend on 35 U.S.C. § 256. *Pannu v. Iolab Corp.*, 155 F.3d 1344, 1349-1350 (Fed. Cir. 1998). Regardless, non-joinder and anticipation fall under different § 102 ***sub-sections*** and state distinct tests: non-joinder asks whether the patentee "did not himself invent" the claimed subject matter, whereas anticipation asks whether one reference discloses every claim element.

obviousness contentions do not turn on the previously-litigated Kiuchi reference. In any event, a claim can be obvious without being anticipated (indeed, that is typically the case), and the public's "paramount interest in seeing that patent monopolies … are kept within their legitimate scope" favors treating each invalidity defense as a separate "issue" for preclusion purposes. *Medtronic v. Mirowski Family Ventures, LLC*, 571 U.S. 191, 203 (2014). And while true that "'invalid patents [should be] declared invalid as early as possible'" (Br. 58), defendants already have a strong incentive to raise their best invalidity arguments early. VirnetX's rule would require defendants to litigate "***every possible*** invalidity theory as opposed to pursuing a streamlined defense," leading to increased "litigation costs," "more complicated" trials, and waste of "judicial resources." *Orexo*, 2019 WL 1177715, at *8.

Finally, VirnetX contends that Apple "actually litigated" its obviousness and non-joinder defenses. Br. 59-61. The district court made no such finding, nor did VirnetX suggest this argument below. Appx16333 (arguing only actual litigation of "anticipat[ion] by the Kiuchi reference"). Indeed, VirnetX's argument contrasts starkly with its assertion only pages later that infringement by iMessage was ***not*** actually litigated in this case, where "neither party ever put forward any arguments or evidence regarding iMessage" at trial. Br. 63. The district court's grant in the 417 Action of a pre-verdict Rule 50(a) motion for judgment on invalidity defenses

not presented to the jury (Br. 59-60) changes nothing; a judgment was entered regarding § 101 in *Voter Verified* too, yet this Court held issue preclusion inapplicable because "'[a] judgment is not conclusive in a subsequent action as to issues which might have been but were not litigated and determined in the prior action.'" 887 F.3d at 1383 (quoting Restatement (Second), Judgments, § 27 cmt. e). Moreover, the district court rejected VirnetX's post-trial request in the 417 Action to "enter judgment on all of Apple's invalidity defenses and counterclaims … which Apple asserted up to the time of trial, ***but never presented to the jury***," concluding that it "will not enter judgment upon claims and defenses ***that were not presented for consideration by the jury***." Appx22395-22396. There is thus no basis for holding that any non-anticipation invalidity issues were "actually litigated" in the 417 Action.

VirnetX's discussion of the non-joinder defense (Br. 59-60) is no more persuasive. The district court's summary judgment turned entirely on the procedural decision to exclude Dr. Schulzrinne's presentation as untimely; "[w]ithout the Schulzrinne presentation," the court found no triable issue. Appx25486. Such a procedural ruling is not "actual and adversarial litigation" of the non-joinder defense. *Regions Hosp. v. Shalala*, 522 U.S. 448, 463-464 (1998).

IV. VIRNETX'S ELEVENTH-HOUR COVENANT NOT TO SUE MOOTS THE iMESSAGE APPEAL.

As Apple explained (Br. 58-61), the district court erred by declining to grant JMOL of non-infringement as to iMessage. The issue remained live because VirnetX pressed its iMessage claim until shortly before trial, Apple maintained its non-infringement counterclaim, and even after trial VirnetX would not agree to dismiss its claim or covenant not to sue Apple.

Without warning or consultation, VirnetX appended a covenant not to sue to its appeal brief in a last-minute attempt to moot the issue. Br. 62 & Ex. 1. VirnetX provides no explanation for its delay. Nevertheless, on the understanding that the covenant applies to all iMessage versions essentially the same as those accused of infringing, Apple agrees that this covenant resolves the issue. And because VirnetX relies on the covenant "to defeat [Apple's] declaratory judgment claim[]," that understanding is "binding [on VirnetX] as a matter of judicial estoppel" in all future actions. *Organic Seed Growers & Trade Ass'n v. Monsanto Co.*, 718 F.3d 1350, 1358 (Fed. Cir. 2013).

VirnetX alternatively contends that Apple abandoned its request for declaratory judgment. Br. 62-65. The district court made no such finding. VirnetX points to only Apple's counsel's response to the court's question about time needed for opening statements. Appx1007 ("I noticed that … iMessage … has been dropped from the case. Is that correct? So the parties won't need as

much time. Is that right?"). Apple's reply—"That's right, Your Honor," and "with the iMessage dropping out, that should be plenty of time" (*id.*)—in no way abandoned Apple's iMessage counterclaim; it simply indicated that VirnetX's decision not to present iMessage-related evidence would shorten the time needed for openings.[14]

CONCLUSION

The judgment should be reversed, or vacated and remanded.

Respectfully submitted,

/s/ William F. Lee

WILLIAM F. LEE
MARK C. FLEMING
LAUREN B. FLETCHER
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-5000

Attorneys for Defendant-Appellee Apple Inc.

BRITTANY BLUEITT AMADI
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Avenue NW
Washington, DC 20006
(202) 663-6000

THOMAS G. SPRANKLING
WILMER CUTLER PICKERING
HALE AND DORR LLP
950 Page Mill Road
Palo Alto, CA 94304
(650) 858-6000

April 5, 2019

[14] VirnetX also contends the iMessage ruling can be affirmed because it is "'clear that the [district court] would have declined to exercise its discretionary jurisdiction." Br. 65 & n.8. But VirnetX points to nothing in the court's cursory analysis evincing any such "clear" intent.

CERTIFICATE OF SERVICE

I hereby certify that, on this 5th day of April 2019, I filed the foregoing Non-Confidential Reply Brief for Defendant-Appellant Apple Inc. with the Clerk of the United States Court of Appeals for the Federal Circuit via the CM/ECF system, which will send notice of such filing to all registered CM/ECF users.

/s/ William F. Lee
WILLIAM F. LEE
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(g), the undersigned hereby certifies that this brief complies with the type-volume limitation of Federal Circuit Rule 32(a).

1. Exclusive of the exempted portions of the brief, as provided in Fed. R. App. P. 32(f) and Fed. Cir. R. 32(b), the brief contains 6,988 words.

2. The brief has been prepared in proportionally spaced typeface using Microsoft Word 2010 in 14 point Times New Roman font. As permitted by Fed. R. App. P. 32(g), the undersigned has relied upon the word count feature of this word processing system in preparing this certificate.

/s/ William F. Lee
WILLIAM F. LEE
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000

April 5, 2019