

No. 2019-1050

---

IN THE  
**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  
Case Nos. 6:12-cv-855-RWS, 6:11-cv-563-RWS, Judge Robert Schroeder, III

---

**CORRECTED NON-CONFIDENTIAL BRIEF FOR APPELLEES  
VIRNETX INC. AND LEIDOS, INC.**

---

Bradley Wayne Caldwell  
Jason Dodd Cassady  
John Austin Curry  
CALDWELL CASSADY & CURRY  
2101 Cedar Springs Road  
Dallas, TX 75201  
(214) 888-4848 (telephone)  
(214) 888-4849 (fax)

Jeffrey A. Lamken  
*Counsel of Record*  
MOLOLAMKEN LLP  
600 New Hampshire Avenue, N.W.  
Washington, D.C. 20037  
(202) 556-2000 (telephone)  
(202) 556-2001 (fax)  
jlamken@mololamken.com

*Counsel for VirnetX Inc.*  
*(Additional Counsel Listed on Inside Cover)*

---

Michael G. Pattillo, Jr.  
Lucas M. Walker  
Rayiner I. Hashem  
James A. Barta  
MOLOLAMKEN LLP  
The Watergate, Suite 660  
600 New Hampshire Ave., N.W.  
Washington, D.C. 20037  
(202) 556-2000 (telephone)  
(202) 556-2001 (fax)

Lauren F. Dayton  
Jennifer E. Fischell  
MOLOLAMKEN LLP  
430 Park Avenue  
New York, NY 10022  
(212) 607-8160 (telephone)  
(646) 710-4945 (fax)

Allison M. Gorsuch  
MOLOLAMKEN LLP  
300 North LaSalle Street  
Chicago, IL 60654  
(312) 450-6700  
(312) 450-6701

*Counsel for VirnetX Inc.*

Donald Urrabazo  
URRABAZO LAW, P.C.  
2029 Century Park East  
Suite 1400  
Los Angeles, CA 90067  
(310) 388-9099 (telephone)  
(310) 388-9088 (fax)

*Counsel for Leidos, Inc.*

**UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT**

VirnetX Inc. v. Apple Inc.

Case No. 19-1050

**CERTIFICATE OF INTEREST**

Counsel for the:

(petitioner)  (appellant)  (respondent)  (appellee)  (amicus)  (name of party)

**VirnetX Inc.**

certifies the following (use "None" if applicable; use extra sheets if necessary):

1. Full Name of Party Represented by me	2. Name of Real Party in interest (Please only include any real party in interest NOT identified in Question 3) represented by me is:	3. Parent corporations and publicly held companies that own 10% or more of stock in the party
VirnetX Inc.	VirnetX Inc.	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:

Ahmad Zavitsanos Anaipakos Alavi & Mensing PC: Jason Scott McManis  
 Caldwell Cassady & Curry, PC: Bradley W. Caldwell, Christopher S. Stewart, Daniel R. Pearson, Hamad M. Hamad, Jason Dodd Cassady, John Austin Curry, John Franklin Summers, Justin Thomas Nemunaitis, Warren Joseph McCarty, III  
 McKool Smith: Douglas A. Cawley, Mitchell Reed Sibley, Ryan Abbott Hargrave, Samuel Franklin Baxter, Stacie Greskowiak McNulty  
 Parker Bunt & Ainsworth, P.C.: Charles Ainsworth, Robert Christopher Bunt, Robert M. Parker, Thomas John Ward, Jr.  
 Ward, Smith & Hill, PLLC: Claire Abernathy Henry  
 MoloLamken LLP: Jeffrey A. Lamken; Michael G. Pattillo, Jr.; Lucas M. Walker; Rayiner I. Hashem; James A. Barta; Allison M. Gorsuch; Jennifer E. Fischell, Lauren F. Dayton

FORM 9. Certificate of Interest

Form 9  
Rev. 10/17

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. *See* Fed. Cir. R. 47.4(a)(5) and 47.5(b). (The parties should attach continuation pages as necessary).

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 Sys., Inc., No. 18-1197 (Fed. Cir.);  
VirnetX Inc. v. Cisco Sys., Inc., No. 18-1751 (Fed. Cir.);  
Inter Partes Reexamination Control No. 95/001,679 (USPTO); 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).

3/8/2019

Date

/s/ Jeffrey A. Lamken

Signature of counsel

Jeffrey A. Lamken

Printed name of counsel

Please Note: All questions must be answered

cc: All counsel of record.

Reset Fields

**UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT**

VirnetX Inc. v. Apple Inc.

Case No. 19-1050

**CERTIFICATE OF INTEREST**

Counsel for the:

(petitioner)  (appellant)  (respondent)  (appellee)  (amicus)  (name of party)

Leidos, Inc.

certifies the following (use "None" if applicable; use extra sheets if necessary):

1. Full Name of Party Represented by me	2. Name of Real Party in interest (Please only include any real party in interest NOT identified in Question 3) represented by me is:	3. Parent corporations and publicly held companies that own 10% or more of stock in the party
Leidos, Inc.	Leidos, Inc.	Leidos Holdings, Inc.

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:

Urrabazo Law, P.C.: Donald Urrabazo, Joon Song, Ronald Wielkopolski, Art Padilla  
MT2 Law Group: Andy Tindel

FORM 9. Certificate of Interest

Form 9  
Rev. 10/17

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. *See* Fed. Cir. R. 47.4(a)(5) and 47.5(b). (The parties should attach continuation pages as necessary).

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 Sys., Inc., No. 18-1197 (Fed. Cir.);  
VirnetX Inc. v. Cisco Sys., Inc., No. 18-1751 (Fed. Cir.);  
Inter Partes Reexamination Control No. 95/001,679 (USPTO); 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).

3/8/2019

Date

/s/ Donald Urrabazo

Signature of counsel

Donald Urrabazo

Printed name of counsel

Please Note: All questions must be answered

cc: All counsel of record

Reset Fields

**TABLE OF CONTENTS**

	<u>Page</u>
STATEMENT OF ISSUES .....	1
STATEMENT OF THE CASE.....	1
I. Technological Background.....	2
A. Internet Addresses and Domain Name Services .....	2
B. Private Networks and VPNs.....	4
C. The Inventors Overcome the Problem of Making Secure Internet Communication User-Friendly .....	6
II. The Patents-in-Suit .....	7
A. The '135 and '151 Patents: A System To Automatically Establish VPN Connections (VPN on Demand).....	7
B. The '504 and '211 Patents: A Secure DNS System That Facilitates Establishing Secure Communication Links (FaceTime) .....	9
III. Proceedings Below .....	11
A. The -417 Case.....	11
B. The -855 Case.....	13
C. The Consolidated Trial.....	13
D. The Renewed -417 Case.....	14
E. The Renewed -855 Case Underlying This Appeal.....	14
1. Trial Evidence—VPN on Demand .....	14
2. Trial Evidence—FaceTime .....	17
3. Verdict and Post-Trial Motions .....	22
SUMMARY OF ARGUMENT .....	24

ARGUMENT .....	27
I. The Jury Properly Found That Redesigned VPN on Demand Infringes the '135 and '151 Patents.....	27
A. Redesigned VPN on Demand Infringes .....	27
1. Redesigned VPN on Demand “Determines” Whether a Query “Is Requesting Access to a Secure Web Site” .....	28
2. Redesigned VPN on Demand “Automatically Initiates” a VPN .....	29
B. Apple’s Non-Infringement Arguments Lack Merit .....	30
C. Apple Is Liable for Infringement .....	34
1. Direct and Induced Infringement of the '135 Patent .....	35
2. Direct Infringement of the '151 Patent.....	39
D. Apple’s Damages Objection Fails.....	40
II. The Jury Properly Found That Redesigned FaceTime Infringes the '504 and '211 Patents.....	41
A. Apple’s Objection to the District Court’s Instruction on “Domain Name Service System” Fails .....	42
1. Apple Failed To Request Its Preferred Claim Construction .....	42
2. The District Court’s Construction Was Correct .....	45
3. Apple Has Not Shown Prejudice .....	47
B. FaceTime Provides the Claimed “Indication”.....	49
III. Apple Is Precluded From Relitigating Validity.....	53
A. The Issue of Validity Was Resolved in the -417 Case.....	53



B.	Apple Actually Litigated Obviousness and Non-Joinder in the -417 Case.....	59
IV.	Apple Is Not Entitled to a Declaratory Judgment of Non-Infringement as to iMessage.....	61
A.	Apple’s iMessage Counterclaim Is Moot.....	62
B.	The District Court Properly Declined To Enter Declaratory Judgment.....	62
V.	Apple’s Remaining Arguments Are Unavailing .....	65
	CONCLUSION.....	66

**CONFIDENTIAL MATERIAL OMITTED**

Material has been redacted in the Non-Confidential Brief for Appellees VirnetX Inc. and Leidos, Inc. The material omitted from page 29 contains information regarding the internal operation of Apple software, which is covered by the protective order entered by the district court on June 24, 2013. Dkt. 55.

**TABLE OF AUTHORITIES**

Page(s)

**CASES**

*Alcon Research Ltd. v. Barr Labs., Inc.*,  
745 F.3d 1180 (Fed. Cir. 2014) .....63, 64

*Already, LLC v. Nike, Inc.*,  
568 U.S. 85 (2013).....62

*Apotex Inc. v. Pfizer, Inc.*,  
125 F. App’x 987 (Fed. Cir. 2005) .....62

*Applied Med. Res. Corp. v. U.S. Surgical Corp.*,  
352 F. Supp. 2d 1119 (C.D. Cal. 2005) .....55

*ArcelorMittal v. AK Steel Corp.*,  
856 F.3d 1365 (Fed. Cir. 2017) .....62

*Arthrocare Corp. v. Smith & Nephew, Inc.*,  
406 F.3d 1365 (Fed. Cir. 2005) .....38

*Broadcom Corp. v. Qualcomm Inc.*,  
543 F.3d 683 (Fed. Cir. 2008) .....35, 38, 39

*Catalina Lighting, Inc. v. Lamps Plus, Inc.*,  
295 F.3d 1277 (Fed. Cir. 2002) .....34

*Comaper Corp. v. Antec, Inc.*,  
596 F.3d 1343 (Fed. Cir. 2010) .....57

*Connell v. Sears, Roebuck & Co.*,  
722 F.2d 1542 (Fed. Cir. 1983) .....57

*Crossroads Sys. (Texas), Inc. v. Dot Hill Sys. Corp.*,  
No. A-03-CA-754-SS, 2006 WL 1544621  
(W.D. Tex. May 31, 2006).....54, 55

*Dana v. E.S. Originals, Inc.*,  
342 F.3d 1320 (Fed. Cir. 2003) .....54, 58, 61

*Del Mar Avionics, Inc. v. Quinton Instrument Co.*,  
836 F.2d 1320 (Fed. Cir. 1987) .....57

*Eli Lilly & Co. v. Aradigm Corp.*,  
376 F.3d 1352 (Fed. Cir. 2004) .....42

*Environ Prods., Inc. v. Furon Co.*,  
215 F.3d 1261 (Fed. Cir. 2000) .....47

*ePlus, Inc. v. Lawson Software, Inc.*,  
700 F.3d 509 (Fed. Cir. 2012) .....37

*Evonik Degussa GmbH v. Materia Inc.*,  
53 F. Supp. 3d 778 (D. Del. 2014).....55

*Finisar Corp. v. DirecTV Grp., Inc.*,  
523 F.3d 1323 (Fed. Cir. 2008) .....27

*Finjan, Inc. v. Secure Computing Corp.*,  
626 F.3d 1197 (Fed. Cir. 2010) .....5, 39, 40

*Ford Motor Co. v. United States*,  
811 F.3d 1371 (Fed. Cir. 2016) .....65

*Hallco Mfg. Co. v. Foster*,  
256 F.3d 1290 (Fed. Cir. 2001) .....58

*Johns Hopkins Univ. v. CellPro, Inc.*,  
152 F.3d 1342 (Fed. Cir. 1998) .....57

*Kennametal, Inc. v. Ingersoll Cutting Tool Co.*,  
780 F.3d 1376 (Fed. Cir. 2015) .....59

*Liberty Ammunition, Inc. v. United States*,  
835 F.3d 1388 (Fed. Cir. 2016) .....46

*Liebel-Flarsheim Co. v. Medrad, Inc.*,  
358 F.3d 898 (Fed. Cir. 2004) .....47

*Lucent Techs., Inc. v. Gateway, Inc.*,  
580 F.3d 1301 (Fed. Cir. 2009) .....35, 37, 38

*Macsentis v. Becker*,  
237 F.3d 1223 (10th Cir. 2001) .....41

*MedImmune, Inc. v. Genentech, Inc.*,  
549 U.S. 118 (2007).....64, 65

*MercExchange, L.L.C. v. eBay, Inc.*,  
401 F.3d 1323 (Fed. Cir. 2005) .....57

*New Hampshire v. Maine*,  
532 U.S. 742 (2001).....53

*O2 Micro Int’l Ltd. v. Beyond Innovation Tech. Co.*,  
449 F. App’x 923 (Fed. Cir. 2011) .....38

*Pall Corp. v. Fisher Sci. Co.*,  
962 F. Supp. 210 (D. Mass. 1997).....55

*PPG Indus., Inc. v. Valspar Sourcing, Inc.*,  
679 F. App’x 1002 (Fed. Cir. 2017) .....62

*Santopadre v. Pelican Homestead & Sav. Ass’n*,  
937 F.2d 268 (5th Cir. 1991) .....60, 61

*Smith & Nephew, Inc. v. Ethicon, Inc.*,  
276 F.3d 1304 (Fed. Cir. 2001) .....32

*Streck, Inc. v. Research & Diag. Sys.*,  
665 F.3d 1269 (Fed. Cir. 2012) .....64

*Sulzer Textil A.G. v. Picanol N.V.*,  
358 F.3d 1356 (Fed. Cir. 2004) .....48

*VirnetX Inc. v. Apple Inc.*,  
No. 6:12-cv-855 (E.D. Tex. Nov. 6, 2012).....13

*VirnetX Inc. v. Cisco Sys., Inc.*,  
748 F. App’x 332 (Fed. Cir. 2019) .....*passim*

*VirnetX Inc. v. Cisco Sys. Inc.*,  
No. 6:10-cv-417 (E.D. Tex. Aug. 11, 2010).....11

*VirnetX, Inc. v. Cisco Sys., Inc.*,  
767 F.3d 1308 (Fed. Cir. 2014) .....*passim*

*Voter Verified, Inc. v. Election Sys. & Software LLC*,  
887 F.3d 1376 (Fed. Cir. 2018) .....55, 56, 60

*Voter Verified, Inc. v. Premier Election Sols., Inc.*,  
698 F.3d 1374 (Fed. Cir. 2012) .....56

*Water Techs. Corp. v. Calco Ltd.*,  
850 F.2d 660 (Fed. Cir. 1988) .....38

*Wilton v. Seven Falls Co.*,  
515 U.S. 277 (1995).....65

*XpertUniverse, Inc. v. Cisco Sys., Inc.*,  
No. 17-CV-03848-RS, 2018 WL 2585436  
(N.D. Cal. May 8, 2018) .....55

*Zip Dee, Inc. v. Dometic Corp.*,  
905 F. Supp. 535 (N.D. Ill. 1995).....55

**STATUTES**

35 U.S.C. § 101 .....56

35 U.S.C. § 102 .....56, 57, 58

35 U.S.C. § 102(f) ..... 11

35 U.S.C. § 103 .....56, 57

35 U.S.C. § 282 .....55

**OTHER AUTHORITIES**

Fed. R. Civ. P. 50(a).....*passim*

Fed. R. Civ. P. 50(a)(1).....60

Restatement (Second) of Judgments § 27 (1982).....54

## STATEMENT OF RELATED CASES

Pursuant to Federal Circuit Rule 47.5, Plaintiff-Appellee VirnetX Inc. states:

a. This case, arising from *VirnetX Inc. v. Apple Inc.*, No. 6:12-cv-855 (E.D. Tex.), has never been appealed to this Court or any other appellate court.

This Court has previously heard two appeals in a related case. The first was *VirnetX, Inc. v. Cisco Sys., Inc.*, No. 13-1489, decided September 16, 2014 and reported at 767 F.3d 1308 (Prost, C.J., and Chen, J.). The second was *VirnetX Inc. v. Cisco Sys., Inc.*, No. 18-1197, decided January 15, 2019 by affirmance without opinion, 748 F. App'x 332 (per curiam) (Prost, C.J., Moore and Reyna, JJ.).

b. The following cases before this Court involve the patents at issue in this appeal: *VirnetX Inc. v. Cisco Sys., Inc.* (No. 18-1751); *VirnetX Inc. v. Apple Inc.* (Nos. 17-1591, -1592, -1593); *VirnetX Inc. v. The Mangrove Partners Master Fund Ltd.* (Nos. 17-1368, -1383); and *VirnetX Inc. v. Iancu* (Nos. 17-2593, -2594).

The following U.S. Patent and Trademark Office (“PTO”) proceedings involve the patents at issue in this appeal: *Apple Inc. v. VirnetX Inc.*, Control Nos. 95/001,788, 95/001,789, 95/001,682, 95/001,697; *Cisco Sys. Inc. v. VirnetX Inc.*, Control Nos. 95/001,851, 95/001,856, 95/001,679, 95/001,714; *Black Swamp IP, LLC v. VirnetX, Inc.*, IPR Nos. 2016-00693, 2016-00957; *The Mangrove Partners Master Fund Ltd. v. VirnetX Inc.*, IPR No. 2015-01046; and *The Mangrove Partners Master Fund Ltd. v. VirnetX Inc.*, IPR No. 2015-01047.

### **STATEMENT OF ISSUES**

1. Whether the jury's finding that redesigned VPN on Demand infringes the '135 and '151 patents is supported by substantial evidence.
2. Whether the jury permissibly found that redesigned FaceTime infringes the '504 and '211 patents.
3. Whether issue preclusion barred Apple from relitigating the validity of patent claims it unsuccessfully challenged in a prior action.
4. Whether the district court properly denied Apple a declaratory judgment on its non-infringement counterclaim for iMessage after Apple abandoned that counterclaim.

### **STATEMENT OF THE CASE**

This case involves patented technology for automatically creating secure communication links over the Internet. In today's hyper-connected world, secure communications are essential. Consumers and businesses use computers and smartphones to exchange highly sensitive information, from private calls with family to details of unannounced corporate mergers. They rely on their devices to prevent hackers from intercepting those communications. Methods for secure communications—such as virtual private networks (“VPNs”)—existed in the prior art, but were cumbersome to use. VirnetX's patented technology overcomes that difficulty, allowing secure links to be created easily and automatically.



VirnetX has accused two Apple features, VPN on Demand and FaceTime, of infringing its patents. Over the course of two actions spanning eight years of litigation, VirnetX has obtained four jury verdicts against Apple. In an earlier appeal, this Court affirmed portions of the first verdict—upholding the patents’ validity and finding infringement as to VPN on Demand—but remanded for a new trial on damages and on infringement by FaceTime. *VirnetX, Inc. v. Cisco Sys., Inc.*, 767 F.3d 1308 (Fed. Cir. 2014) (“*VirnetX I*”). Following two more trials, this Court affirmed the jury’s verdict on infringement and damages for VPN on Demand and FaceTime alike. *VirnetX Inc. v. Cisco Sys., Inc.*, 748 F. App’x 332 (Fed. Cir. 2019) (“*VirnetX II*”).

This case arises because, after the first verdict against it, Apple changed VPN on Demand and FaceTime in an effort to avoid infringement. A jury found those revised versions infringe as well. Apple now seeks to overturn that verdict.

## **I. TECHNOLOGICAL BACKGROUND**

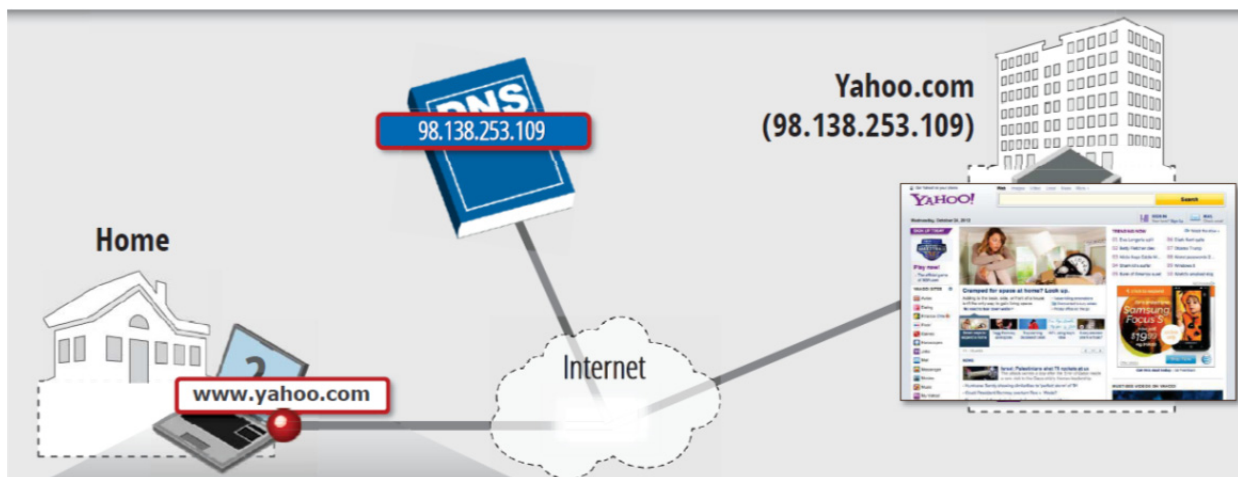
### **A. Internet Addresses and Domain Name Services**

The Internet is a global communications network comprising myriad interconnected devices, such as PCs, smartphones, and servers. Appx1208-1209. Computers on the Internet communicate by sending “packets” of data through a network of specialized devices (“routers”). Appx1209-1210. Packets are passed

from router to router until the data eventually reaches its intended destination. *Id.*  
In that way, any computer on the Internet can communicate with any other. *Id.*

Each Internet device is assigned a numerical “IP address,” such as “172.217.15.110.” Appx1210. Computers and routers use IP addresses to deliver packets toward and to their destinations. *Id.*

IP addresses, however, are inconvenient for *people* to use. Domain name services (“DNS”) thus allow users to identify a computer on the Internet using a “domain name,” such as “yahoo.com.” Appx1209-1210. As shown below, when a user types “yahoo.com” into a web browser, the user’s computer queries a DNS to find the IP address for Yahoo!’s server (“98.138.253.109”). The computer then uses that IP address to communicate with the server and retrieve the Yahoo! web page. *Id.*



Appx10003.

The Internet is fundamentally unsecure. Routers are not controlled by a trusted central authority; consequently, packets are vulnerable to interception by eavesdroppers. Appx1209-1210. Moreover, by inspecting the IP addresses in the packets, hackers can learn about the identities of the communicating parties. Appx2287.

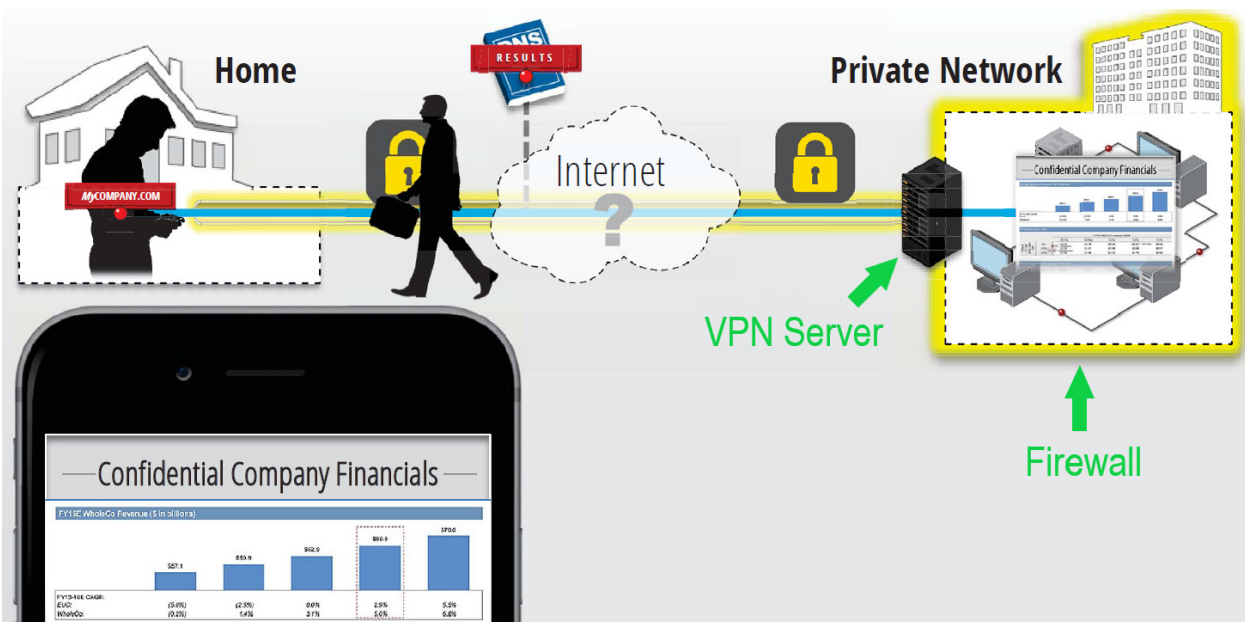
**B. Private Networks and VPNs**

Apart from the Internet, there are *private* computer networks, like those inside corporate offices, that limit access to authorized users and devices. Appx1210-1211. Because access is controlled, computers on such networks typically can communicate with each other without additional security measures. Appx1217; Appx1282.

Private networks are often connected to the Internet—say, to allow employees to exchange emails with people outside the company. Appx1210-1211. Special devices called “firewalls” are interposed between the private network and the Internet, allowing computers within the private network to access the Internet while preventing malicious access to the private network from outside. *Id.*

Nonetheless, users outside a firewall often need to access computers behind the firewall. For example, telecommuting employees may need documents stored on their company’s private server. Appx1237-1238. VPNs enable a device outside the private network (“client device”) to access a device inside the private

network by creating a *secure* communication link over the otherwise unsecure Internet. Appx1211; Appx1217-1218; Appx1343-1345. The client device connects to a “VPN server” at the edge of the private network, which acts as a secure gateway through the firewall. Appx1345-1346. The client device and VPN server use data encryption to ensure that anyone intercepting their communications cannot decipher the contents. Appx1351.



Appx10004 (green annotations added; irrelevant portion omitted). VPNs can also provide a degree of anonymity by encrypting certain IP addresses. Appx1342-1344; *VirnetX I*, 767 F.3d at 1318.

While VPNs enable secure Internet communication, in the prior art they “were notoriously difficult” to use. Appx1545. Network administrators had to set up both the client device and the VPN server, configuring dozens of settings and

establishing encryption “keys” to allow exchange of coded information. *Id.* As a result, users often did not use VPNs available to them—putting their data at risk. Appx1561-1562.

**C. The Inventors Overcome the Problem of Making Secure Internet Communication User-Friendly**

The inventors—Robert Short, Edmund Munger, Douglas Schmidt, Victor Larson, and Michael Williamson—confronted the VPN difficulty-of-use problem while developing secure-communications technology for the U.S. military. Appx1206. As secure military satellites became overwhelmed by a flood of data (*e.g.*, real-time battlefield imagery), the military needed to transmit its sensitive data through untrusted commercial satellites. Appx1206-1207. To that end, the inventors created a highly secure VPN called “netEraser.” Appx1208, Appx1211-1212. Like other contemporary VPNs, however, netEraser was hard to use. Appx1212-1213; *see* Appx1545-1546. That exacerbated risks: “if security was complicated, people weren’t going to use it.” Appx1213.

To solve the difficulty-of-use problem, the inventors looked at how users access resources on the Internet. To reach a website, users type a domain name, such as “yahoo.com.” The user’s device consults a DNS to find the site’s IP address and connect to it. *See* p. 3, *supra*. The inventors realized that a special system placed “in the middle of that process” could be used to “determine if the user or the application is asking for a secure domain connection” and (if so)

establish a VPN link automatically without requiring users to “change their behavior.” Appx1215. The inventions here (detailed in Section II) followed from that insight. They make it easy “for the average user . . . to have safe, secure connections automatically.” Appx1198.

The inventors realized their inventions were perhaps most useful for commercial settings. Appx1220-1221. Because their employer did not make consumer products, they went to work for VirnetX. Appx1228, Appx1232. There they developed a commercial software product called “Gabriel” that allowed secure communication over the Internet. Appx1235-1236.

## **II. THE PATENTS-IN-SUIT**

The inventors obtained patents for their new technologies. Appx1222, Appx1228. The patents-in-suit are U.S. Patent Nos. 6,502,135 (’135 patent), 7,490,151 (’151 patent), 7,418,504 (’504 patent), and 7,921,211 (’211 patent).

### **A. The ’135 and ’151 Patents: A System To Automatically Establish VPN Connections (VPN on Demand)**

The ’135 and ’151 patents share a common specification. They describe a system “that transparently creates a virtual private network in response to a domain name inquiry.” Appx172, 32:33-35; *see* Appx305, 6:7-9. (Here, “transparently” means the process of creating a VPN is invisible to the user. Appx175, 38:1-13.)

Ordinarily, when a user tries to access a public Internet site using a domain name, the device will send a request to a DNS to find the public IP address of the

corresponding computer. *See* p. 3, *supra*. (The patents refer to ordinary public DNS servers as “conventional” DNS servers. Appx175, 37:22-29.) The disclosed system, however, examines such “DNS lookup” requests to “determine[] whether access to a secure site has been requested.” Appx175, 38:23-28. For example, it might check the requested domain name against an “internal table” of secure sites. *Id.*, 38:27-28. If access to a secure site has *not* been requested, the system “‘passes through’ the request” to the conventional DNS, which returns an IP address that can be used to create an ordinary, unsecured link. *Id.*, 38:6-11.

If the user *is* trying to access a secure site, the system seeks to establish a VPN link. It checks “whether the user has sufficient security privileges to access the site.” Appx175, 38:28-32. If so, it creates “a virtual private network . . . between [the] user computer . . . and [the] secure target site.” *Id.*, 38:30-32. The invention also “facilitates the allocation and exchange of information needed to communicate securely”—information that users previously had to configure manually. *Id.*, 38:53-60; *see* pp. 5-6, *supra*.

Independent claim 1 and dependent claim 7 of the ’135 patent cover the operation of the system described above. Claim 1 recites:

A method of transparently creating a virtual private network (VPN) between a client computer and a target computer, comprising the steps of:

- (1) generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer;

- (2) determining whether the DNS request transmitted in step (1) is requesting access to a secure web site; and
- (3) in response to determining that the DNS request in step (2) is requesting access to a secure target web site, automatically initiating the VPN between the client computer and the target computer.

Appx180.

Claim 7 addresses the exchange of information needed to communicate securely. Appx180. Claim 13 of the '151 patent is directed to a computer-readable medium containing code for a system that automatically creates a VPN link in response to a query for a secure site, or passes the request through to a conventional DNS if the requested site is not a secure site. Appx325-326.

**B. The '504 and '211 Patents: A Secure DNS System That Facilitates Establishing Secure Communication Links (FaceTime)**

The '504 and '211 patents share a common specification. They disclose a specialized “secure DNS” system that enables “‘one-click’ and ‘no-click’ technique[s]” for “establishing a secure communication link between” two computers over the Internet without “entering any cryptographic information.” Appx237, 6:28-30, 6:40-48.

The preferred embodiment “contains a cross-reference database of secure domain names and corresponding secure network addresses.” Appx260, 51:11-12. That registry allows users to find other devices by domain name. *Id.*, 51:15-16. When a user tries to find another device, the system “authenticates the query” to verify the requesting device’s identity. *Id.*, 51:51.



The system also “facilitates the allocation and exchange of information,” such as encryption keys, “needed to communicate securely.” Appx254, 40:37-40. Once one device has that information, it can initiate a secure communication link to the other. Appx260, 51:62-64. Consequently, “[t]he user does not need to enter any user identification information, passwords or encryption keys for establishing a secure communication link.” Appx259, 50:19-21. All further communication occurs over that secure link. Appx260, 51:67-52:1.

Independent claim 1 and dependent claims 2, 5, and 27 of the '504 patent claim the secure DNS system. Claim 1 is representative:

A system for providing a domain name service for establishing a secure communication link, the system comprising:

a domain name service system configured

- [1] to be connected to a communication network,
- [2] to store a plurality of domain names and corresponding network addresses,
- [3] to receive a query for a network address, and
- [4] to comprise an indication that the domain name service system supports establishing a secure communication link.

Appx262 (line breaks and numbers added).

The '211 patent is similar. The asserted claims, independent claim 36 and dependent claims 47 and 51, differ primarily in that they are directed to machine-

readable media comprising the instructions for implementing the DNS system claimed in the '504 patent. Appx402.

### **III. PROCEEDINGS BELOW**

This appeal arises from the second of two actions accusing certain features of Apple's iOS devices (*e.g.*, iPhones) of infringing VirnetX's patents. In both cases, VirnetX accused Apple's "VPN on Demand" feature of infringing the '135 and '151 patents, and Apple's "FaceTime" feature of infringing the '504 and '211 patents. In the first action—the -417 case—juries found the patents valid and infringed by *original* versions of VPN on Demand and FaceTime. Over the course of two appeals, this Court agreed.

In this action—the -855 case—a jury found infringement by *revised* versions of VPN on Demand and FaceTime. Apple now appeals a third time.

#### **A. The -417 Case**

VirnetX filed its first complaint in 2010, alleging infringement by then-existing versions of VPN on Demand and FaceTime. *VirnetX Inc. v. Cisco Sys. Inc.*, No. 6:10-cv-417 (E.D. Tex. Aug. 11, 2010) (" -417 case"), Appx25007-25010. Apple filed a counterclaim challenging each asserted claim as invalid. Appx25383.

Apple lost two invalidity arguments—non-joinder and derivation under pre-AIA § 102(f)—at summary judgment. Apple alleged that Dr. Henning Schulzrinne

had conceived the inventions and disclosed them to the inventors in a presentation, Appx25402-25403, but the district court held Apple's evidence was insufficient to create a triable question. Appx25486. Just before trial, Apple sought to dismiss its remaining invalidity arguments, including obviousness and anticipation. Appx25487-25490; Appx25575-25592. The court refused, and the case proceeded to trial in October 2012. Appx25591-25592; *see* Appx25450-25454.

Near the close of evidence, Apple announced it would argue only anticipation based on a reference called Kiuchi. Appx25980-25982. VirnetX moved for judgment under Rule 50(a) on all other invalidity arguments Apple had "announced ready for trial" but not supported with evidence, including obviousness. Appx25503-25505; Appx26107-26109. With Apple's assent, the district court entered "judgment as a matter of law on theories of invalidity, other than anticipation over the Kiuchi reference[,] as to the asserted claims." Appx26113; *see* Appx25523. The jury rejected Apple's anticipation argument; found all four patents valid and infringed; and awarded VirnetX \$368 million in damages. Appx25525-25526.

Apple appealed, but did not challenge the disposition of any invalidity argument other than anticipation. This Court affirmed the jury's findings on validity and infringement by VPN on Demand, but remanded on certain

infringement issues regarding FaceTime and for a new trial on damages. *VirnetX I*, 767 F.3d at 1313-14, 1334.

**B. The -855 Case**

After the adverse verdict in the -417 case, Apple released new versions of VPN on Demand and FaceTime. VirnetX filed a new infringement action (“-855 case”)—the one underlying this appeal. *VirnetX Inc. v. Apple Inc.*, No. 6:12-cv-855 (E.D. Tex. Nov. 6, 2012).

In particular, VirnetX accused a version of VPN on Demand released in September 2013 (“redesigned VPN on Demand”) of infringing claims 1 and 7 of the ’135 patent and claim 13 of the ’151 patent. It also accused a version of FaceTime released in September 2013 (“redesigned FaceTime”) of infringing claims 1, 2, and 27 of the ’504 patent and claims 36, 47, and 51 of the ’211 patent. Those same claims had been asserted and found valid in the -417 case. Appx25525-25526. VirnetX separately alleged that another iOS feature, iMessage, infringed the ’504 and ’211 patents. Appx26223-26249, ¶¶ 14-74.

**C. The Consolidated Trial**

The -855 case was initially tried together with the issues this Court remanded in the -417 case. Appx26260-26261. The jury again ruled for VirnetX, awarding \$625 million in damages. Appx15619-15624. Afterward, the district court concluded the joint trial had prejudiced Apple. Appx15625; *see* Appx26329.

The court severed the cases and set both for new, separate trials. Appx15625-15639.

**D. The Renewed -417 Case**

In September 2016, the district court held a third trial limited to the issues this Court remanded in the -417 case: infringement by original FaceTime and damages (including for original VPN on Demand). *See* Appx25556. The jury returned a third verdict for VirnetX and awarded over \$300 million in damages. Appx25559-25560. Apple again appealed. This Court affirmed. *VirnetX II*, 748 F. App'x 332.

**E. The Renewed -855 Case Underlying This Appeal**

While *VirnetX II* was pending before this Court, this case (the -855) against redesigned VPN on Demand and FaceTime went to trial for a second time. Before trial, the district court granted VirnetX partial summary judgment on Apple's invalidity defenses, holding that issue preclusion barred Apple from relitigating the validity of claims it had unsuccessfully challenged in the -417 action. Appx1.

1. *Trial Evidence—VPN on Demand*

At trial, VirnetX's expert, Dr. Jones, explained how Apple's new "Evaluate Connection" mode of VPN on Demand infringes the '135 and '151 patents. (Apple introduced that mode after the prior "Always" mode was found to infringe in the -417 case.) "Evaluate Connection" mode operates differently depending on

whether the user's device is inside or outside a particular firewall. Appx1332-1334.

Whenever an Apple device with VPN on Demand connects to a new network, it sends out a "probe" to determine whether the user is inside the firewall of a given private network (*e.g.*, the user's office network). Appx1332-1334; Appx2243; Appx5040-5043. The firewall probe tries to access a designated server accessible *only* within that private network. Appx1332-1334. If the probe succeeds, VPN on Demand knows the user is on the private network, inside the firewall. If it fails, that means a firewall is between the user and any server on that private network. *Id.*; Appx2391. The result of the probe "is held [stored] somewhere on the device" and affects how VPN on Demand operates. Appx2244.

If the user's device is *outside* the firewall, VPN on Demand will attempt to create a VPN link whenever the user requests access to a secure resource. Appx1334-1335. When the user selects a domain name, VPN on Demand simultaneously (a) checks the domain name against a configured list of secure domain names, and (b) forwards a request for the requested domain name to a traditional DNS server. Appx1335-1336; *see* Appx2245-2247. If the requested domain name matches an entry in the list, VPN on Demand automatically creates a VPN link to the corresponding secure resource, and the response from the conventional DNS server is discarded. Appx1335-1338; *see* Appx2245-2247. If

the requested domain name does not match, VPN on Demand uses the IP address returned by the conventional DNS to establish an ordinary, unsecured link. Appx1335-1338.

If the user is *inside* the firewall, VPN on Demand establishes an ordinary, non-VPN link to the requested resource. Appx1337-1338. Because the user's device is inside the same firewall as the requested resource, additional security from a VPN is unnecessary. Appx1338.

VPN on Demand operates as follows when presented with a domain-name request in "Evaluate Connection" mode:

<b>Firewall Probe Result</b>	<b>Requested Domain Name Found in List?</b>	<b>Conventional DNS Query Result</b>	<b>VPN on Demand Link Type</b>
Outside firewall	Yes	Discarded	<i>VPN link</i>
Outside firewall	No	IP address of corresponding site	Unsecured link
Inside firewall	Yes	IP address of corresponding site	Unsecured link
Inside firewall	No	IP address of corresponding site	Unsecured link

Dr. Jones explained how VPN on Demand's "Evaluate Connection" mode meets each claim limitation. Appx1339-1352. Most relevant here, he explained that VPN on Demand "determin[es]" whether a DNS request generated by a user's iOS device "is requesting access to a secure web site." Appx1340-1341. It does so by "checking that the domain name . . . [in the] DNS request matches one of the

names” on the configured list of secure domains, and by “checking the results of the [firewall] probe,” since a user outside a site’s firewall “requires authorization for access.” Appx1341; Appx1348. Where those checks show that access to a secure site is requested, VPN on Demand “automatically initiat[es] the VPN between the client computer and the target computer” “without the user having to do anything” else. Appx1342-1343.

Apple’s expert, Dr. Blaze, “agree[d]” with Dr. Jones about redesigned VPN on Demand’s “basic operation.” Appx2373; *see* Appx2374. In Dr. Blaze’s view, however, the feature does not infringe because it does not initiate a VPN link based on whether the user has requested access to a secure site, but instead looks to the user’s “location.” Appx2352. Dr. Blaze nevertheless 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. Appx2393; *see* Appx2246 (Apple employee admitting same). Apple’s own engineer admitted that, when a device is outside the firewall, “Evaluate Connection” mode “replicate[s]” old VPN on Demand’s “Always” mode—which the parties agreed infringes. Appx1387-1388; Appx1463.

## 2. *Trial Evidence—FaceTime*

FaceTime enables secure communications, such as video calls, between two iOS devices. To make a call, the caller selects the intended callee using the



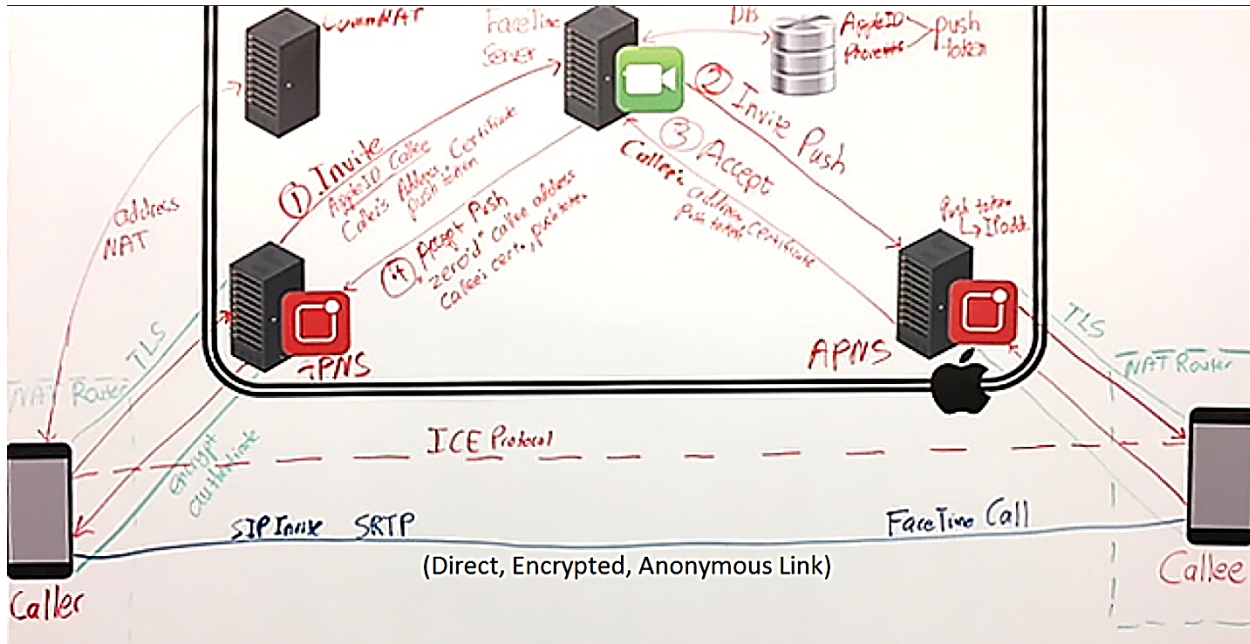
callee's Apple ID or phone number. Appx1357-1358. Apple's FaceTime servers then undertake a "provisioning process [that] includes authenticating the identities of both of the parties and their phones" and "providing the information that allows the parties to communicate with each other securely." Appx1376-1378; *see* Appx1358-1363. As Dr. Jones explained, this process involves four sequential messages between the devices and FaceTime's servers:

1. Invite. The caller's device sends FaceTime's servers an "Invite" message that includes (among other things) the callee's Apple ID, the caller's IP address, and a cryptographic "certificate" proving the caller's identity. Appx1358-1359. The FaceTime server verifies the caller's identity and performs other verifications. Appx1359.

2. Invite Push. After authenticating the caller, the FaceTime server locates the callee in a list of registered FaceTime users and sends the callee an "Invite Push" message. Appx1360. That message includes the caller's IP address, certificate, push token, and session token. Appx1360-1361. Once the Invite Push arrives, the callee can accept or reject the call.

3. Accept. If the callee device accepts the call, it sends FaceTime's servers an "Accept" message containing the callee's address, a certificate proving the callee's identity, tokens, and other information. Appx1361.

4. Accept Push. FaceTime's servers send the caller's device an "Accept Push" message containing the callee's certificate and other information, such as push tokens. Appx1362. The Accept Push does not include the callee's actual IP address, but instead returns a string of zeroes ("0.0.0.0.") in its place. *Id.*



Appx10001 (showing four push messages and direct link) (annotation added).

Through this exchange, FaceTime's servers provide the callee with the caller's IP address, and provide both the caller and the callee with certificates verifying identities. That information enables the devices to exchange information directly (a process called the "ICE protocol"). Appx1362-1363. Using the caller's IP address, the callee sends data packets to the caller. Using the certificate received in the Accept Push, the caller confirms those packets are from the intended callee. The packets give the caller the callee's IP address, allowing the

caller to respond to the callee and agree on encryption keys. Appx1363. Finally, the caller device initiates an encrypted, direct communication link with the callee for the exchange of video and audio data. Appx1363-1364.

Dr. Jones explained how FaceTime practices each limitation of the '504 and '211 patents. Appx1373-1385. Most relevant here, he addressed the limitation that the system “comprise *an indication* that the domain name service system *supports establishing a secure communication link.*” Appx1374-1376 (emphasis added). He explained that the link between caller and callee is a “secure communication link” because it is direct, encrypted, and anonymous. Appx1372. FaceTime “supports establishing” that link by providing address and security information necessary for direct communications and by facilitating concealment of the parties’ IP addresses. *Id.*; Appx1375-1379. Finally, the Accept Push is an “indication” that the system supports establishing a secure communication link because it notifies the caller that the provisioning process has been completed, as well as supplying information needed to enable the encrypted direct link. Appx1378.

Dr. Blaze did not dispute Dr. Jones’s explanation of how FaceTime works. Appx2400; *see* Appx2295-2297. Instead, he based his non-infringement opinion on differences between original FaceTime (found to infringe in the -417 case) and redesigned FaceTime. He explained that in original FaceTime the Accept Push

contained the callee's IP address, which the caller used to initiate a direct link with the callee. Appx2297. In redesigned FaceTime, the Accept Push does *not* provide the callee's IP address to the caller. Instead, the *callee* "learns the IP address of the sender" from the Invite Push. Appx2301. That allows the *callee* to send its own IP address to the caller, which in turn enables the caller to initiate a direct link. *Id.*<sup>1</sup>

Dr. Blaze testified that removal of the callee's IP address from the Accept Push precludes infringement. Appx2301; Appx2321-2322. In his view, the claimed "indication" must *itself* "return a network address" to the caller, to allow *the caller* to immediately initiate a direct link. Appx2411; *see* Appx2426-2430 (urging that claims require the "IP address be sent to the caller, not the callee, and that the caller and not the callee initiate the direct communication"); Appx2410. Dr. Blaze acknowledged that the court's claim construction did not require the "indication" to include an IP address. Appx2426-2430.

---

<sup>1</sup> In a short-lived intervening version of FaceTime, Apple removed *both* the callee's IP address from Accept Push *and* the caller's IP address from Invite Push. Appx2297; Appx1479. Because neither party had the other's IP address, it was impossible for either to initiate a direct link. Appx1479-1481. All FaceTime calls therefore connected using a fallback method that exchanged data *indirectly* through a relay server. Appx2298-2299. Because the communication link was not "direct," the parties agreed that intervening version of FaceTime was noninfringing. Appx1479-1481.

### 3. *Verdict and Post-Trial Motions*

The jury returned a verdict for VirnetX, finding that Apple infringed each asserted claim, that it did so willfully, and that VirnetX was entitled to \$502 million in damages. Appx50-52; Appx64-65. The district court denied Apple's motions for judgment as a matter of law and for a new trial.

VPN on Demand. Apple urged that redesigned VPN on Demand does not infringe because it does not create a VPN link “in response to” “determining whether a DNS request . . . is requesting access to a secure web site.” Instead, Apple insisted, it decides whether to start a VPN based on the user's location—inside or outside a firewall—not on the “DNS request.” Appx79-82. The district court disagreed. The evidence showed VPN on Demand “performs this determination by comparing the domain name of the DNS request against a list of domain names in a configuration file *and* by consulting the result of the [firewall] probe.” Appx81 (emphasis added). “This evidence satisfies the [c]ourt's claim constructions,” it explained, because “whether the requesting device is inside or outside” the firewall “affects whether a server *requires authorization for access* (which is a requirement of the [c]ourt's construction of ‘secure server’).” Appx81-82.

The district court rejected Apple's argument that VirnetX failed to prove actual use of an infringing configuration. Appx85-88. The court noted that the apparatus claim requires only the *capability* for infringing use. Appx85-86. As to

the method claims, the court credited VirnetX's evidence that "Evaluate Connection" mode could "replicate" original VPN on Demand's infringing "Always" mode. Appx86-87. Given the "customer backlash" Apple faced when it tried to remove "Always" mode, the jury could have inferred that customers who used that mode configured new VPN on Demand to operate the same way. Appx87. The court also pointed to Apple test plans supporting infringement by Apple itself. Appx88.

FaceTime. The district court rejected Apple's challenges to the FaceTime verdict. Apple challenged the court's instruction that the claim term "domain name service system" did not incorporate the court's construction of the separate term "domain name service." Appx76-77; Appx98-99. The court explained that it had repeatedly ruled that the "claim language itself provides a description of the domain name service system"—*i.e.*, one configured to carry out the steps identified in the claims. Appx76-77. And it found that Apple had not explained "what prejudice [it] suffered from the [c]ourt explaining the nuances of its claim construction to the jury." Appx99.

Apple also argued that FaceTime did not infringe because the alleged "indication"—the Accept Push—did not contain the callee's IP address. Appx73. The court disagreed, explaining that its claim construction "requires an indication *other than* the mere return of an IP address, so return of an IP address is not

required.” Appx74 (emphasis added). It sufficed that the Accept Push included other information—such as “the callee’s certificate, a peer-push token, session token, a certificate name for the callee”—that “indicates that the FaceTime servers have successfully authenticated and provisioned both devices to establish a direct, secure FaceTime call.” Appx75. The court rejected Apple’s contention that a direct link cannot be created when the Accept Push does not include the callee’s IP address. Appx74.

iMessage. Finally, Apple sought a declaratory judgment of non-infringement as to iMessage. VirnetX had initially accused iMessage but dropped that contention shortly before trial. Appx89. Apple, in turn, had affirmed to the district court that iMessage was “dropping out,” Appx1007, and did not present any evidence or argument on its non-infringement counterclaim at trial. The court declined to “enter judgment on claims and defenses that were not presented for consideration to the jury.” Appx89.

### **SUMMARY OF ARGUMENT**

I.A. Substantial evidence supports the jury’s finding that redesigned VPN on Demand infringes. VPN on Demand “determin[es] whether access to a secure server has been requested” by checking the requested domain against a list of secure domains and checking whether the server is behind a firewall. If so, it “automatically” creates a VPN “in response.”

B. Contrary to Apple’s arguments, checking whether a server is located behind a firewall is *part* of “determining” whether a secure server is requested, as a server behind a firewall requires authorization for access. Even if it were not, the inclusion of an additional step does not defeat infringement where, as here, all claimed steps are performed.

C. Sufficient evidence showed actual use of the infringing configuration. As to the method claims, Apple created, tested, and encouraged customer testing of the infringing mode as a replacement for its concededly infringing “Always” mode. The jury could reasonably infer that customers who relied on “Always” mode used its replacement the same way, as Apple encouraged. The apparatus claims are infringed by the presence of software code to perform the claimed functions, even without actual use.

D. Apple’s argument that damages should have been reduced to account for supposedly limited infringement is waived and meritless. Apple never objected to VirnetX’s damages testimony on that basis, and its own expert made no such adjustment. Further, every accused product infringes the apparatus claims, and there was ample evidence of the infringing capability’s value.

II. The jury properly found that redesigned FaceTime infringes.

A. Apple’s objection to the jury instruction that the claimed “domain name service system” does not incorporate the construction of “domain name



service” is waived and wrong. Apple never sought its preferred construction. And the district court correctly concluded the terms are distinct. The instruction, moreover, provided appropriate clarification and caused no prejudice.

B. Substantial evidence showed FaceTime comprises an “indication” that it “supports establishing a secure communication link.” FaceTime “supports” creating a secure, direct link by authenticating the parties’ identities and providing information needed for the link. It “indicates” such support in an Accept Push message signaling the successful culmination of that process.

Apple complains that the Accept Push does not contain the callee’s IP address. But the claims do not require it to do so. Nor does that render direct communications impossible. Redesigned FaceTime gives the caller’s IP address to the callee, which allows the callee to reach the caller and (after further direct exchanges) allows the caller to initiate a direct link. Apple’s comparison to a non-infringing version of FaceTime fails because that version supported only *indirect* calls.

III. Issue preclusion barred Apple from relitigating the validity of claims it unsuccessfully challenged in the -417 case. Apple protests that it seeks to raise different invalidity theories than before, but overwhelming authority holds that validity is a single “issue” for preclusion purposes. This Court’s precedent does

not suggest otherwise. In any event, while Apple now seeks to argue obviousness and non-joinder, it litigated—and lost on—those theories in the -417 case.

IV. Apple’s request for a declaratory judgment of non-infringement as to iMessage is moot because VirnetX has covenanted not to sue for iMessage’s infringement of the asserted patents. Moreover, the district court properly denied Apple’s request after Apple abandoned its iMessage counterclaim before trial.

V. Apple’s arguments contingent on other cases are premature. Should later rulings implicate this case, supplemental briefing may be appropriate.

### **ARGUMENT**

#### **I. THE JURY PROPERLY FOUND THAT REDESIGNED VPN ON DEMAND INFRINGES THE ’135 AND ’151 PATENTS**

##### **A. Redesigned VPN on Demand Infringes**

An infringement verdict must be affirmed unless “no reasonable jury could have found infringement.” *Finisar Corp. v. DirecTV Grp., Inc.*, 523 F.3d 1323, 1333 (Fed. Cir. 2008). Based on his review of Apple’s source code, Dr. Jones cogently explained how the “Evaluate Connection” mode of Apple’s redesigned VPN on Demand practices each claim element. Appx1330-1343.

Apple contests (at 32-39) only two claim limitations. It insists redesigned VPN on Demand does not “determin[e]” whether a DNS query “is requesting access to a secure web site.” It also disputes whether, when a request is for a “secure web site,” redesigned VPN on Demand “automatically” establishes a VPN.

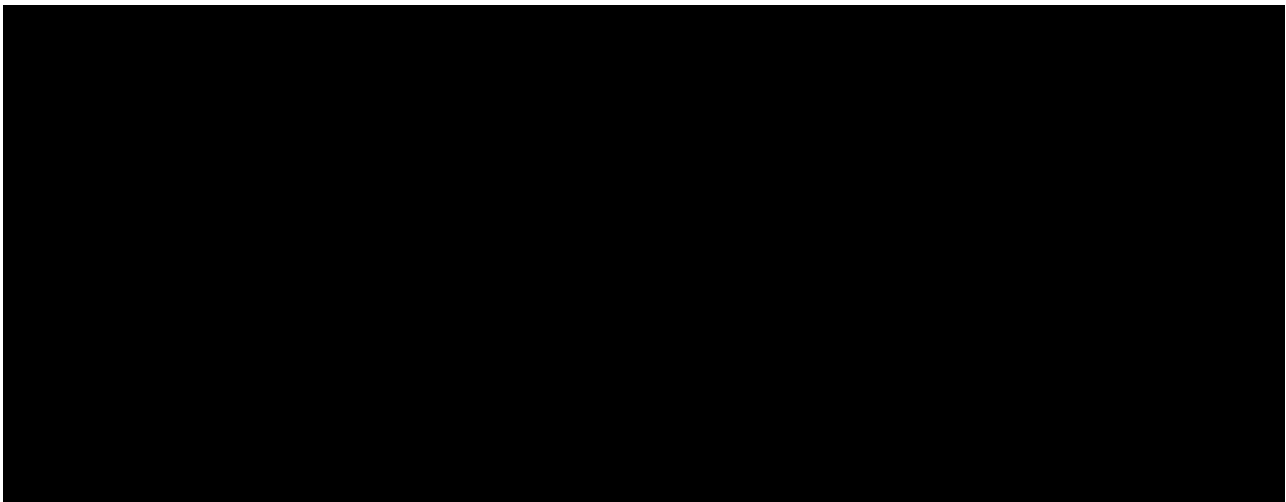
But Dr. Jones showed how redesigned VPN on Demand meets both limitations. It “determin[es]” whether a query is for a “secure web site” by checking whether the requested domain name is in a list of secure domains and whether there is a firewall between the user’s device and the requested site. Appx1340-1341. If the request is for a secure site, VPN on Demand establishes a VPN link “automatically”—“without the user having to do anything” else. Appx1343.

1. *Redesigned VPN on Demand “Determines” Whether a Query “Is Requesting Access to a Secure Web Site”*

Redesigned VPN on Demand “determin[es]” whether a query “is requesting access to a secure web site” or “secure server.” Appx180, cl.1; Appx326, cl.13; Appx1340-1342; Appx1347-1348. The parties agreed that a “secure” website or server is one that “requires authorization for access” and “can communicate in a VPN” or encrypted channel. Appx15046; Appx15065. “Evaluate Connection” mode performs the claimed determination by checking those two characteristics.

VPN on Demand “check[s]” whether the requested domain name “matches” a list of secure domains configured by an IT administrator. Appx1341; *see* Appx2246; Appx2700. A match indicates that the corresponding server “can communicate in a VPN.” Appx1341; *see* Appx2700. Checking against the domain-name list thus serves to “determine” whether access to a secure site has been requested, Appx1341; Appx2700, as this Court recognized in *VirnetX I*, 767 F.3d at 1320.

VPN on Demand also checks whether there is a firewall between the user and the requested server, using the results of its firewall probe. Appx1341; pp. 15-16, *supra*. The “usual technique” for restricting access to a server is to place it behind a firewall. Appx2334. If a server is behind a firewall, the user “can’t reach” it “without authorization.” Appx1341; *see* Appx81-82; Appx1348-1349; Appx2196-2197; Appx2334; Appx2698-2699. Accordingly, the fact that a server is “behind a firewall . . . tend[s] to imply that it is a *secure server*.” Appx2248 (emphasis added); *see* Appx2378-2379.



Appx5055 (highlighting added).

2. *Redesigned VPN on Demand “Automatically Initiates” a VPN*

Redesigned VPN on Demand also “automatically initiat[es]” a VPN when it determines a request is for a secure site. Appx180, cl.1; *see* Appx326, cl.13. The parties agreed that “automatically initiating” a VPN means “initiating the VPN without involvement of a user.” Appx15046.

Redesigned VPN on Demand does precisely that. If it “determines” that a secure site is requested, it creates a VPN without the “user having to do anything” further. Appx1343; *see* Appx2719, Appx5055 (user input precedes decision to create VPN). And it does so “in response to determining that the DNS request . . . is requesting access to a secure target site.” Appx180, cl.1; *see* Appx326, cl.13. As explained above (at 25-29), both the domain-list matching and the firewall probe are used to “determine” whether a request is for a secure server. VPN on Demand initiates a VPN as a result of those checks being satisfied. *See* Appx5055 (Apple flowchart showing “Start VPN” operation occurs when the requested “[h]ostname matches” the “domain list” and the “probe fails” (*i.e.*, the user is outside the firewall)).

**B. Apple’s Non-Infringement Arguments Lack Merit**

Apple argues (at 32-39) that redesigned VPN on Demand does not “automatically initiat[e]” a VPN “in response to determining” that access to a secure site is being requested. That is so, Apple says, because redesigned VPN on Demand does not create a VPN whenever the requested site’s domain is on the list of secure domains, but only when the firewall probe shows “the requesting device is outside the firewall.” Apple Brief 37. That argument is doubly flawed.

1. First, the firewall probe is *part* of determining whether access is being requested to a secure site, as Dr. Jones explained. Appx1341-1349. The parties

agreed that a “secure server” is one requiring “authorization for access,” and that servers behind a firewall require “authorization for access.” Appx15046; Appx1484-1485; *see* Appx2248; Appx2378-2379. Accordingly, a device *outside* the firewall may require authorization (via a VPN) to access a server on the private network. But, as this Court explained in *VirnetX I*, devices inside a private network are already protected by physical security; they generally will not need further authorization to access network resources. 767 F.3d at 1321. Simply put, to someone outside the network, the network is secure *because* they must traverse the firewall.

Apple dismisses the probe as a “location check” that has nothing to do with access to a secure server. But the system does not care where the user is situated in the abstract; it cares whether the user must traverse a firewall—a security barrier—to access network resources. Apple scoffs at the notion that “a server can be both secure and non-secure, depending on the requesting device’s location,” Apple Brief 37-38, but the concept is hardly novel. The contents of a bank vault are secure as to people outside the vault, but not those standing inside it.

Apple’s reliance on *VirnetX I* (at 33, 36) is misplaced. This Court held that domain-list matching in old VPN on Demand satisfied the “determining” limitation. 767 F.3d at 1320. It did not, as Apple suggests, hold that domain-list matching was the *only* way to satisfy that limitation. As the foregoing makes

clear, checking whether a firewall stands between the user and a server *also* serves to determine whether that server is “secure.”

2. Second, even if the firewall probe were not part of the claimed “determining” step, that would not defeat infringement. “Infringement arises when all of the steps of a claimed method are performed, whether or not the infringer also performs additional steps.” *Smith & Nephew, Inc. v. Ethicon, Inc.*, 276 F.3d 1304, 1311 (Fed. Cir. 2001). The claims require initiating a VPN link “in response” to determining that access to a secure site is being requested. “Evaluate Connection” mode satisfies that requirement (even under Apple’s narrow conception of “determining”) because it *always* checks the list of secure domains and, when it creates a VPN link, it does so “in response” to a match. Appx5055 (showing that list matching always occurs). That is enough for infringement, even if addition of the probe means the system might sometimes decline to create a VPN link despite a match. Apple seems to argue that, once a server is determined to be on the domain list, the VPN link must be initiated not just “automatically” but *inexorably*. But “automatically” just means “without involvement of a user,” Appx15046—not always or invariably.

The specification and claim differentiation preclude Apple’s construction. In one embodiment, additional checks are carried out *after* determining that “access to a secure host was requested” but *before* the “VPN is established.”

Appx176, 39:7-20, 39:22-24; *see* Appx151. Similarly, dependent claims 4 and 5 recite adding a security check after the “determinating” step, but “*prior* to automatically initiating the VPN.” Appx180 (emphasis added). Apple’s approach would make those dependent claims impossible.

Finally, the firewall probe is not deployed *after* domain-list matching. The “probe is actually sent when there’s a new network association”—whenever the user switches networks—“before you even drop down into the Evaluate Connection logic” used for deploying VPN on Demand. Appx2243-2244. Once the probe determines the user is outside the firewall, that determination governs later DNS queries. As a result, whenever the user is outside the firewall, creation of a VPN turns *only* on whether the requested domain matches the secure-domain list—not just automatically but inexorably. Appx1335-1337; Appx5055.

3. Because VirnetX agreed Apple’s original “If Needed” mode does not infringe, Apple compares “Evaluate Connection” to that mode. Apple Brief 4, 11-12, 27. “Evaluate Connection” must not infringe, Apple urges, because (like “If Needed”) it “performs a location check and only initiates a VPN if it determines that the requesting device is located outside the secure server’s firewall.” *Id.* at 34. But what Apple characterizes as a “location check” in old “If Needed” is actually a conventional DNS query. *See* Appx27797. Whether a domain name is found in a conventional DNS has nothing to do with whether a user is inside or outside a



particular firewall—as Apple’s own documents show. *See* Appx10063 (server behind a firewall may be listed in conventional DNS).

Besides, the “location check” is not what made old “If Needed” non-infringing. That mode did not infringe because it tried to create an unsecured link to any server found in a conventional DNS, *even if* the domain name appeared in the list of secure domains. Appx27797. It attempted a VPN as a last resort. Non-infringement had nothing to do with “location,” but rather the preference for unsecured links. “Evaluate Connection,” with the probe configured, operates differently. It *always* checks the requested domain against the list of secure domains and will *not* preferentially create unsecured links. Appx5055. And while it performs a conventional DNS query, it discards that result for users outside the firewall—establishing a VPN connection—whenever the requested domain is on the secure list. *Id.* Apple’s comparisons to old “If Needed” are irrelevant.

### **C. Apple Is Liable for Infringement**

Apple itself tested configurations that infringe the ’135 patent. It induced its customers to use those configurations. And it infringed the ’151 patent by selling devices containing code enabling infringement. Appx87-88; Appx1386-1387. Each of those findings independently supports the infringement verdict. *See Catalina Lighting, Inc. v. Lamps Plus, Inc.*, 295 F.3d 1277, 1291 (Fed. Cir. 2002).

1. *Direct and Induced Infringement of the '135 Patent*

When “Evaluate Connection” mode is configured with (1) a list of secure domains with the “ConnectIfNeeded” option, and (2) the “RequiredURLString-Probe” parameter (*i.e.*, the firewall probe) set to any non-empty value, the method claims of the '135 patent are infringed by users. Appx1332-1334.

Direct Infringement by Apple and Its Customers. Apple insists (at 40) there is no evidence “anyone employed” VPN on Demand in the infringing mode. But there was ample “circumstantial evidence” for the jury to find Apple and its customers directly infringed. *Lucent Techs., Inc. v. Gateway, Inc.*, 580 F.3d 1301, 1318 (Fed. Cir. 2009); *Broadcom Corp. v. Qualcomm Inc.*, 543 F.3d 683, 699 (Fed. Cir. 2008).

Apple developed “Evaluate Connection” mode, like the concededly infringing “Always” mode before it, to address customer demands. The first VPN on Demand supported only “If Needed” mode. Appx1330. “If Needed” would create a VPN only when a requested domain was unavailable in a conventional DNS, but that “wasn’t what users wanted or expected it to do.” *Id.* “[P]eople were not happy,” calling it a “broken feature” and “completely busted.” *Id.* “Dual-facing server[s]”—ones behind a firewall also listed in a conventional DNS—presented special problems. Appx2219. “If Needed” would attempt to connect unsecurely to the outward-facing content; as a result, it showed public content when users

expected internal content, or failed to connect altogether. Appx10063. Workarounds were devised. Appx10066-10068; Appx1329-1331. Dissatisfaction was so great, Apple created the infringing “Always” mode to establish VPNs *whenever* the requested domain name was in the list of secure sites. Appx1330-1331.

“Always” mode was so important to customers that Apple could not remove it even after it was found to infringe. When Apple proposed doing so, Eli Lilly, a large customer, complained the change would “render VPN on Demand useless” and begged “Apple not to do this.” Appx1388; *see* Appx10070. The technology press excoriated the proposal. Appx10066. Apple ultimately retained “Always” mode until it developed “Evaluate Connection” mode—which can “replicate” the infringing “Always” mode using the firewall probe. Appx1332.

Apple intended its customers to use “Evaluate Connection” in just that way. Appx1386. It developed a “VPN on Demand test plan” that involved configuring “Evaluate Connection” mode with (1) a list of secure domain names with the ConnectIfNeeded option, and (2) enabling the firewall probe. Appx10077. The plan stated that it addressed “[d]ual-facing servers,” which “were previously handled” by “Always” mode. Appx10074. Apple’s “Configuration Profile Reference” likewise instructed users to configure VPN on Demand to “replicate” the “Always” functionality. Appx1332-1333; *see* Appx10118-10121. Indeed, the

manual's discussion of the now-removed "Always" mode referred users to instructions for configuring "Evaluate Connection" mode. Appx10115.

That evidence—customer demand for the infringing "Always" mode and Apple's release of a "new version of VPN on Demand, which replicates the Always mode"—was at least "circumstantial evidence" that Apple customers used new VPN on Demand in an infringing configuration. Appx87; *see Lucent*, 580 F.3d at 1318.

The evidence likewise supports a finding that Apple directly infringed. Appx86. The jury could "reasonably have concluded that the" VPN on Demand "test plan was carried out" by Apple's (California-based) engineers. Appx86; Appx1386; Appx2258-2259; Appx2194-2195; *see ePlus, Inc. v. Lawson Software, Inc.*, 700 F.3d 509, 521 (Fed. Cir. 2012) (invoking "circumstantial evidence" of "live testing"). That conclusion is especially reasonable here: Apple was preparing to remove "Always" mode, and the test plan specifically addressed scenarios that had led to customer complaints before that mode's introduction.

Apple asserts (at 41, 42) that the jury relied on "pure speculation" and "hypothetical[]" possibilities. That blinks reality. The customer needs that prompted creation (and retention) of "Always" mode did not disappear when Apple removed that mode, and the test plan makes clear Apple intended "Evaluate Connection" mode—in the infringing configuration—to address scenarios "pre-

viously handled” by “Always” mode. Appx10074. No “unsupported leaps,” Apple Brief 41, are needed to conclude that customers who had used infringing “Always” mode used its infringing replacement for the same reasons. *See Lucent*, 580 F.3d at 1318 (reasonable to infer customer infringement where product was “designed” to practice invention and customers were “instructed” accordingly); *O2 Micro Int’l Ltd. v. Beyond Innovation Tech. Co.*, 449 F. App’x 923, 928 (Fed. Cir. 2011) (“complete certainty” not required).

Apple Induced Customers’ Infringement. There was ample evidence that Apple intended to—and did—induce its customers’ infringement. Inducement requires “that the alleged infringer knowingly induced infringement and possessed specific intent to encourage another’s infringement.” *Broadcom*, 543 F.3d at 697.

Apple designed “Evaluate Connection” mode, with the firewall probe, to “replicate” the infringing “Always” mode. *See pp. 35-37, supra*. That is an act of inducement. *See Water Techs. Corp. v. Calco Ltd.*, 850 F.2d 660, 668 (Fed. Cir. 1988). Apple also instructed users to configure VPN on Demand in the infringing mode—another act of inducement. *See Arthrocare Corp. v. Smith & Nephew, Inc.*, 406 F.3d 1365, 1377 (Fed. Cir. 2005). Apple, moreover, possessed “specific intent.” *Broadcom*, 543 F.3d at 701. As the district court explained, “Apple knew about the patents-in-suit before the redesign, knew that the previous version

infringed, and replicated that original design.” Appx90.<sup>2</sup> And Apple’s test plan makes clear Apple intended users to configure VPN on Demand in an infringing manner. *See* pp. 36-37, *supra*.

## 2. *Direct Infringement of the ’151 Patent*

Regardless, Apple directly infringes the ’151 patent. Claim 13 is addressed to a “computer readable medium storing” computer “instructions that, when executed, cause” the computer to perform a method similar to those claimed in the ’135 patent. Appx326. Such *Beauregard* claims are infringed where the “program code for” performing the infringing function “is ‘literally present’ on all accused products.” *Finjan, Inc. v. Secure Computing Corp.*, 626 F.3d 1197, 1205 (Fed. Cir. 2010). As Dr. Jones explained, Apple infringed by selling iOS devices containing VPN on Demand code corresponding to the software components disclosed in claim 13. Appx1347-1352.

Apple argues there is no infringement because the firewall probe is “disabled by default” and requires configuration to operate. Apple Brief 44. But *every* VPN on Demand mode requires configuration. *See VirnetX I*, 767 F.3d at 1315; Appx10114-10121. And a need for configuration does not overcome infringement. In *Finjan*, this Court held that software infringed computer-readable-medium

---

<sup>2</sup> Apple cannot argue it did not know redesigned VPN on Demand would infringe. The jury found Apple infringed willfully, and Apple has not appealed that determination. Appx109; *see Broadcom*, 543 F.3d at 699.

claims even where the relevant functionality was disabled until “customers purchased keys and unlocked” it. 626 F.3d at 1203. What mattered was that “software for performing the claimed functions existed in the products when sold.” *Id.* at 1205. That is true here: To perform the claimed functions, all that is required is setting up a configuration file according to Apple’s instructions. *See* pp. 36-37, *supra*. No “software” need be altered. *Contra* Apple Brief 44.

Apple contends (at 44) that the usual rules for computer-readable-medium claims do not apply because claim 13 requires actual “execution.” Not so. Claim 13 requires only that the computer perform certain operations “when executed.” Appx326. It is indistinguishable from the claims this Court found infringed in *Finjan*. Those claims too “recite[d] software components . . . ‘for causing’ a server . . . to perform certain steps” when executed. 626 F.3d at 1205.

#### **D. Apple’s Damages Objection Fails**

Apple argues (at 46) that VirnetX’s damages expert, Mr. Weinstein, should have reduced his reasonable royalty estimate to account for the fact that VPN on Demand only infringes in certain modes.

That argument is waived. Apple never sought to exclude Mr. Weinstein’s testimony on that basis. *See* Appx26256-26258. Presumably that was because Apple’s expert *also* calculated damages based on a uniform per-unit royalty without adjustment for the frequency of infringement. Appx2530-2593. Apple

first raised its objection to that methodology after evidence closed, under Rule 50(a). That was too late. *See Macsenti v. Becker*, 237 F.3d 1223, 1233-34 (10th Cir. 2001).

Apple's argument also fails on the merits. For one thing, *every* Apple product infringed the computer-readable-medium claims. For another, the jury heard that the infringing "functionality is important to users." Appx1389. They heard that customers considered the prior "If Needed" mode "broken" and "useless," with impacts on large companies. Appx1331; Appx1338. Apple presented no contrary testimony, and its own damages calculation did not adjust for supposedly limited infringement. The jury was entitled to conclude that the infringing "Evaluate Connection" mode (like the prior "Always" mode) was sufficiently valuable to Apple to warrant a per-unit royalty.

## **II. THE JURY PROPERLY FOUND THAT REDESIGNED FACETIME INFRINGES THE '504 AND '211 PATENTS**

The jury heard extensive evidence that redesigned FaceTime meets each limitation of the asserted '504 and '211 claims. Appx1372-1379. Apple's non-infringement arguments fixate on a single fact: that FaceTime's Accept Push message does not provide the callee's IP address to the caller. Apple argues that, as a result, FaceTime cannot be a "domain name service system" and cannot "comprise an indication that the domain name service system supports establishing a



secure communication link.” Apple Brief 46-55. But neither the claims nor technology require return of an IP address to the caller.

**A. Apple’s Objection to the District Court’s Instruction on “Domain Name Service System” Fails**

While Apple begins by objecting to the district court’s instructions, it is really arguing claim construction. Apple contends that the term “domain name service system” should incorporate the requirements for a conventional “domain name service,” which “returns an IP address for a requested domain name to the requester.” Apple Brief 46-47 (quoting Appx22214). But Apple never timely requested its “must-return-an-IP-address” construction of “domain name service system.” And the court properly instructed the jury in any event.

1. *Apple Failed To Request Its Preferred Claim Construction*

A litigant that “never requested that the district court construe any terms in [a claim] and never offered a construction of [the] claim” until “after the presentation of all of the evidence to the jury” has “waived its right to request a claim construction.” *Eli Lilly & Co. v. Aradigm Corp.*, 376 F.3d 1352, 1360 (Fed. Cir. 2004). In this case, Apple *never* requested a construction of “domain name service system”—much less one that incorporates the construction of “domain name service” or requires return of an IP address. *See* Appx26172 (claim construction chart). The district court’s *Markman* order thus did not address the term,

even as it construed terms like “domain name” and “Domain Name Service.” Appx15064.

Apple later attempted to disqualify VirnetX’s expert because he had not opined that FaceTime is a “domain name service.” Appx15149. That was necessary, Apple suggested, because “domain name service” is “a limitation of the claims as part of the phrase ‘domain name service system.’” Appx26434. But when VirnetX challenged Apple’s position, Appx26263-26264, Apple disclaimed seeking a claim construction, avowing that it did not “intend to revisit any claim construction proposals that were implicitly or explicitly rejected by the [c]ourt,” Appx15591. The court thus ruled that “[t]he construction of ‘domain name service system’ does not incorporate the construction of ‘domain name service’” because “these are two different terms used in different context.” Appx26684.

The court so instructed the jury at trial. Appx85. Even when it objected to that instruction, Apple did not seek the construction of “domain name service system” it now proposes. It argued the instruction was *unnecessary* because it had “*never argued* at any time that ‘domain name service’ is incorporated in ‘domain name service system,’ nor [had it] ever at any time relied on ‘domain name service system’ as the term that gave rise to [its] non-infringement defense.” Appx2639 (emphasis added). Apple’s Rule 50(a) motion did not make those arguments either. *See* Appx26356-26361. Not until its *post-trial* motions did Apple contend

that “domain name service system” should be construed to incorporate the limitations of “domain name service.” Appx16217; Appx16246. The court properly “decline[d] to reconsider its previous rulings” based on that belated submission. Appx76-77.

Apple portrays the court’s construction of “domain name service system” (and accompanying jury instruction) as a surprise. Apple Brief 47. But Apple had ample notice—not just from the proceedings discussed above, but from eight years of litigation. In the -417 case, Apple *did* propose a construction of “domain name service system.” Appx21303. But the court declined to adopt it (or any construction incorporating the definition of “domain name service”). Appx22218. Instead, the court held the term “does not require construction” because “[t]he claim language itself provides a description of the domain name service system”—namely, that “it must ‘comprise an indication that [it] supports establishing a secure communication link.’” Appx22219. The court reaffirmed that view after the first -417 trial: Although it had construed “domain name service,” it “did not construe ‘domain name service system’ because the claim language itself provided a description of the term, i.e. that it must ‘comprise an indication that [it] supports

establishing a secure communication link.’” Appx22364 n.3.<sup>3</sup> Yet Apple never sought a different construction in this (-855) case—even though it sought to revisit *other* claim-construction rulings. See Appx15064 (*Markman* order addressing constructions from -417 case). Apple simply chose not to timely raise the claim-construction argument it presses today.

2. *The District Court’s Construction Was Correct*

The court’s construction was correct. Claim 1 of the ‘504 patent requires:

***a domain name service system*** configured

- [1] to be connected to a communication network,
- [2] to store a plurality of domain names and corresponding network addresses,
- [3] to receive a query for a network address, and
- [4] to comprise an indication that the domain name service system supports establishing a secure communication link.

Appx262 (line breaks, numbers, and emphasis added). As the court recognized, “[t]he claim language itself provides a description of the domain name service system.” Appx22219. The system must ***connect*** to a network, ***store domain names*** and network addresses, ***receive*** network-address queries, and ***comprise an indication*** of support for establishing a secure communication link. Nowhere does

---

<sup>3</sup> While the court found original FaceTime met the “domain name service” limitation in any event, see Appx22364; Apple Brief 49, its opinion made clear the claims did not demand that.

the claim require that it *return an IP address to the requester* as Apple now insists. Apple Brief 47.<sup>4</sup>

The specification, moreover, repeatedly distinguishes the invention from prior-art “conventional DNS server[s]” and “standard domain name service[s].” *See, e.g.*, Appx254, 39:7-49, 39:67-40:1, 40:53-56; Appx259, 50:37-40; Appx260, 51:34-40, 52:6-8, 52:51-55; Appx261, 53:5-8; *cf. Liberty Ammunition, Inc. v. United States*, 835 F.3d 1388, 1399 (Fed. Cir. 2016) (relying on specification’s “distinguish[ing] the claimed invention from” prior art). It makes clear that a conventional DNS is entirely optional. *See* Appx259, 50:45-51 (a network with the claimed “secure domain name service” system “*can* include *other* network services, such as . . . a *standard domain name service*” (emphasis added)). It makes no sense to assume, as Apple does, that the invention must replicate every feature of a conventional DNS.

Apple’s position is particularly untenable given that the asserted claims expressly include some conventional DNS features (like receiving network-address queries) but not others (like returning a network address to the requester). Only *unasserted* dependent claims require returning a network address. Claim 14 requires that the system “*respond* to the query for the network address,” while

---

<sup>4</sup> The claim’s preamble (“A system for providing a domain name service . . .”) also includes the term “domain name service.” Apple conceded below that “the preamble is not a limitation,” Appx2647, and does not rely on it here.

claim 15 requires that the response provide “*the network address* corresponding to a domain name.” Appx262 (emphasis added). Similarly, claim 35 adds a domain-name database “configured so as to *provide a network address* corresponding to a domain name in response to a query in order to establish a secure communication link.” Appx263 (emphasis added). Where a dependent claim “adds a particular limitation,” that limitation is presumptively not part of the independent claim. *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 910 (Fed. Cir. 2004). The district court properly refused to read Apple’s proposed limitation into claims where it does not appear.

### 3. *Apple Has Not Shown Prejudice*

Apple says (at 50-51) it was an abuse of discretion to deliver the instruction even if it was correct. But the instruction was entirely justified, and Apple has not shown prejudice. *See Environ Prods., Inc. v. Furon Co.*, 215 F.3d 1261, 1265 (Fed. Cir. 2000).

Apple’s insistence (at 50) that the instruction was unnecessary is belied by its contention (at 47) that “[t]he claimed ‘DNS system’ *naturally includes* the limitations of the claimed ‘DNS.’” (Emphasis added.) Having taken that position, Apple can hardly deny that jurors instructed to give claim language its “ordinary and accustomed meaning,” Appx2758, might reach the same erroneous conclusion. The district court was entitled to “take steps to assure that the jury un-

derstands that it is not free to consider its own meanings for disputed claim terms.” *Sulzer Textil A.G. v. Picanol N.V.*, 358 F.3d 1356, 1366 (Fed. Cir. 2004).

Moreover, during trial, Dr. Blaze erroneously asserted that the court’s construction of “domain name service” governed and that “the [c]ourt’s constructions . . . require returning an IP address for th[e] requested domain name to the requester.” Appx98; Appx2412. While Dr. Blaze later agreed that “the construction of ‘domain name service system’ does not incorporate the construction of ‘domain name service,’” Appx2421-2422, it was appropriate for the jury to receive clarification from the court. “The jury must be told that the court has made a claim construction ruling that the jury must follow.” *Sulzer Textil*, 358 F.3d at 1366.

Apple says (at 51) the instruction “improperly suggested that the failure to return an IP address could not be a basis for non-infringement.” But the instruction did no such thing. It did not mention IP addresses, much less specify whether one is required to provide an “indication” as a technological matter. It simply informed the jurors—accurately—that they should not plug the construction of “domain name service” into the distinct term “domain name service system.” A well-informed jury is not unfair prejudice.

**B. FaceTime Provides the Claimed “Indication”**

Apple argues (at 51-55) that FaceTime does not “comprise an indication” that it “supports establishing a secure communications link.” Ample evidence showed otherwise.

FaceTime *supports establishing* a secure communication link. It does so through a “provisioning process [that] includes authenticating the identities of both of the parties and their phones” and “providing the information that allows the parties to communicate with one another securely,” such as “certificates for each one of the parties.” Appx1376, 1378. That information enables the two devices to exchange additional data with each other and initiate an encrypted “direct,” “peer-to-peer call.” Appx1362-1364; *see* Appx1372.

FaceTime *indicates* its support for establishing a secure link by returning an Accept Push message to the caller. As Dr. Jones explained, the Accept Push is “the culmination of th[e] provisioning process” just described. Appx1376; Appx72. It tells the caller “the provisioning process has been completed,” such that establishing a secure connection is supported. Appx1378. It also contains information the caller needs to initiate the direct link, including “the callee’s certificate, a push token, [and] a certificate name for the callee.” Appx1376. If the callee declines the call, the Accept Push includes a “reject message” indicating that



FaceTime “will not support . . . establish[ing] a secure communication link in that case.” Appx1383.

Apple’s argument that the Accept Push is not the claimed “indication” rests entirely on the fact that the Accept Push does not include the callee’s IP address. Apple Brief 52. But the claims do not demand that the indication include an IP address. Apple does not contend otherwise. The district court held (at Apple’s request) that the indication must be something “*other than* merely returning . . . an IP address.” Appx15051 (emphasis added). That is what the Accept Push does. It indicates FaceTime’s support for a secure communication link by means *other than returning the callee’s IP address*. See Appx1377-1378 (Accept Push does not merely return conventional DNS records). Apple paraphrases the claim construction as requiring that “the claimed ‘indication’ . . . do *more* than ‘merely’ return an IP address.” Apple Brief 54. But the construction requires only that the indication do something *other than* merely return an IP address, not that it return something *in addition to* an IP address.

Apple contends that, as a *technological* matter, it is impossible to establish a “direct” communication link without the indication providing the caller with the callee’s IP address. Apple Brief 52-53. But FaceTime does just that for millions of direct calls every day. While Apple initially “attempted to conceal” that redesigned FaceTime “support[s] direct peer-to-peer FaceTime calls,” Appx109, it

can no longer deny that direct FaceTime calls happen despite the callee's IP address being absent from the Accept Push. The jury was entitled to credit Dr. Jones's testimony that what actually happens is indeed possible. As he explained, both parties will eventually need each other's IP address for two-way conversation, but "[y]ou don't need IP addresses from both parties to establish [a] direct communication to begin with." Appx1482-1483. It is enough that the *callee* receive the *caller's* IP address, which it does via FaceTime's Invite Push. Appx1482; Appx1479. That enables the callee to send a data packet containing "the callee's IP address" directly to the caller. Appx1482. At that point, each device has the other's IP address and can exchange security keys and other information needed for a direct, secure, two-way call. Appx1362-1364.

Apple protests that this final exchange (the "ICE protocol") "has nothing to do with the accused FaceTime servers or Accept Push message." Apple Brief 53. But the ICE protocol works only because FaceTime's servers provision each device with needed information—including, for example, the callee's certificate in the Accept Push. Appx1362-1363. FaceTime's servers "support" establishing a direct link by providing that information, even if further (direct) exchanges of information between the devices are needed. It is likewise irrelevant that "the caller can't initiate a direct FaceTime call to the callee' 'based on the contents of the [A]ccept [Push] message *alone*.'" Apple Brief 53 (emphasis altered). The

claims require only that the “indication” show *the system* supports establishing a secure link, Appx262—not, as Apple would have it, that *the indication itself* include *every* piece of information used to establish the link.

Apple compares the accused version of FaceTime to a non-infringing version from April 2013. Apple Brief 52-53. But the April 2013 version connected all FaceTime calls *indirectly* through a relay server situated between the two parties. Appx1419-1420; Appx1479. That version did not infringe because it did not support establishing a “direct” communication link (or “indicate” such support). Appx1364-1365; Appx1419-1420. The version accused here supports establishing a direct link—and so infringes. That both the April 2013 version and the revised version “zero out” the callee’s IP address from the Accept Push, *see* Apple Brief 52-53, makes no difference. As Dr. Jones explained, the April 2013 version zeroed out *both* the callee’s IP address (in the Accept Push) *and* the caller’s IP address (in the Invite Push)—preventing direct contact and requiring use of indirect, relayed connections instead. Appx1479-1481. In the revised version, by contrast, the Invite Push provides the caller’s IP address to the callee; the callee sends data packets with its IP address directly to the caller; and the caller device then creates the direct link. Appx1480-1481. The Accept Push also includes the callee’s certificate (missing from the April 2013 version), which allows the caller to verify those packets are from the intended callee. Appx1481-1482. As already

discussed (at 49-50), those features provide—and indicate—support for establishing a secure, direct link.

Finally, Apple quibbles (at 55) that revised FaceTime and its Accept Push also support indirect, relayed calls as a backup. But the same was true of the original version of FaceTime held to infringe in the -417 case. Appx1528-1529. And several items in the Accept Push refer specifically to direct (“peer”) calls. *See* Appx1377 (“peer-push-token”); Appx10020, Appx10023. Apple’s position reduces to this: While FaceTime’s servers indisputably support establishing secure communication links, they somehow fail to indicate as much. That defies common sense—and the evidence at trial.

### **III. APPLE IS PRECLUDED FROM RELITIGATING VALIDITY**

#### **A. The Issue of Validity Was Resolved in the -417 Case**

Issue preclusion prohibits “successive litigation of an issue of fact or law actually litigated and resolved in a valid court determination essential to [a] prior judgment.” *New Hampshire v. Maine*, 532 U.S. 742, 748-49 (2001) (citations omitted). Apple does not contest most of the doctrine’s elements. It does not dispute that the validity of every asserted claim was “actually litigated” in the -417 case. Nor does it dispute that the rejection of its invalidity defense was “essential” to the prior judgment against it. *See* Appx7 (elements undisputed). Apple argues only that the -417 case is not preclusive because the invalidity “issues” (*e.g.*,

anticipation versus obviousness) are different. *See* Apple Brief 57-58 & n.12. The district court correctly rejected that argument.

1. The relevant “issue” for preclusion purposes is “the ultimate determination on patent validity itself, not the sub-issues or the individual pieces of evidence and arguments’” that might bear on that determination. Appx7 (quoting *Crossroads Sys. (Texas), Inc. v. Dot Hill Sys. Corp.*, No. A-03-CA-754-SS, 2006 WL 1544621, at \*5 (W.D. Tex. May 31, 2006)). Because Apple sought to invalidate the same patent claims in both cases, the “validity dispute [was] identical”—even if Apple’s invalidity *theories* might differ. Appx7.

Bedrock preclusion principles support that conclusion. Once an issue is resolved against a party, “new arguments may not be presented to obtain a different determination of that issue.” Restatement (Second) of Judgments §27 cmt. c (1982). Nor may parties escape preclusion by offering “to buttress their case through different evidence.” *Dana v. E.S. Originals, Inc.*, 342 F.3d 1320, 1325 (Fed. Cir. 2003). Yet that is what Apple seeks to do here. Having failed to prove the asserted claims invalid, Apple wants a second bite using arguments (*e.g.*, obviousness) and evidence (different prior art) it hopes will prove more persuasive.

The “‘overwhelming weight of authority’” rejects such tactics. Appx6-7 (quoting *Crossroads*, 2006 WL 1544621, at \*5).<sup>5</sup> Courts have long held that a party’s unsuccessful validity challenge precludes later attacks on the same claim, taking care to distinguish “the *issue* of the validity or invalidity of [a] patent” from “the *arguments* that a party may advance in its effort to prevail on such an issue.” *Zip Dee, Inc. v. Dometic Corp.*, 905 F. Supp. 535, 537 (N.D. Ill. 1995). Invalidity defenses are all rooted in §282 and share a common standard of proof; “new theories of invalidity would require presentation of substantially the same evidence,” namely “comparison of prior art” to the challenged claims; and “discovery and pretrial preparation would reasonably [be] expected to embrace all invalidity arguments.” *Applied Med. Res. Corp. v. U.S. Surgical Corp.*, 352 F. Supp. 2d 1119, 1125 (C.D. Cal. 2005) (applying Restatement (Second) of Judgments factors), *aff’d*, 435 F.3d 1356 (Fed. Cir. 2006). A contrary rule would allow parties to treat validity “like a salami, to be consumed one slice at a time.” *Zip Dee*, 905 F. Supp. at 536 n.1.

Apple asserts that *Voter Verified, Inc. v. Election Sys. & Software LLC*, 887 F.3d 1376 (Fed. Cir. 2018) (“*Voter Verified II*”), “rejected the single-issue

---

<sup>5</sup> See also, e.g., *Evonik Degussa GmbH v. Materia Inc.*, 53 F. Supp. 3d 778, 793 (D. Del. 2014) (collecting cases); *XpertUniverse, Inc. v. Cisco Sys., Inc.*, No. 17-CV-03848-RS, 2018 WL 2585436, at \*4 (N.D. Cal. May 8, 2018); *Pall Corp. v. Fisher Sci. Co.*, 962 F. Supp. 210, 213 (D. Mass. 1997).

approach to invalidity.” Apple Brief 56. Not so. *Voter Verified II* concerned two *different* requirements for issue preclusion. It held that the prior rejection of a defendant’s § 101 invalidity defense was not preclusive in a later case because (1) the invalidity issue “was not necessary to the judgment” in the first case, as the defendant prevailed on non-infringement grounds; and (2) the “issue was not actually litigated” in the prior case, as the defendant “failed to present any arguments or evidence” of any sort “regarding invalidity.” 887 F.3d at 1379, 1383. The Court did not consider whether § 101 subject-matter eligibility is the “same issue” as patentability under §§ 102 and 103. The defendant had lost on *all* of those invalidity theories in the first case because it “fail[ed] to present any argument or evidence.”” *Voter Verified, Inc. v. Premier Election Sols., Inc.*, 698 F.3d 1374, 1379, 1381-82 (Fed. Cir. 2012); see *Voter Verified II*, 887 F.3d at 1379-80. None of those theories had been “actually litigated,” so none could be preclusive.

2. Even if *Voter Verified II* held that “invalidity challenges under §§ 102 and 103” present a different issue from “a § 101 challenge”—and it did not—that would not help Apple. Apple Brief 56. Apple offers no principled basis for treating anticipation under § 102 (which it litigated in the -417 case) and obviousness under § 103 (which it seeks to litigate now) as different issues for preclusion purposes. Anticipation and obviousness involve not merely the same *issue* (invalidity) but fundamentally the same *argument*—that prior art renders a

claim unpatentable. As this Court has long recognized, ““anticipation is the epitome of obviousness.”” *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548 (Fed. Cir. 1983). For that reason, “a disclosure that anticipates under § 102 also renders the claim invalid under § 103,” *id.*, while an obviousness argument can encompass anticipation, *see MercExchange, L.L.C. v. eBay, Inc.*, 401 F.3d 1323, 1330 (Fed. Cir. 2005) (obviousness argument preserved anticipation argument), *vacated on other grounds*, 547 U.S. 388 (2006); *Johns Hopkins Univ. v. CellPro, Inc.*, 152 F.3d 1342, 1357 n.21 (Fed. Cir. 1998) (party permissibly argued anticipation in a new trial on obviousness). A party that litigates one theory effectively litigates the other.

Apple’s only response is that anticipation and obviousness are “under different statutory sections.” Apple Brief 57. But it cannot explain why that matters. Nor can it justify the arbitrary results its approach would produce. Under Apple’s proposed rule, its failure to prove the claims were *anticipated* by Kiuchi would not preclude it from arguing that the claims are rendered *obvious* by Kiuchi, viewed with the knowledge of one skilled in the art. *Cf. Comaper Corp. v. Antec, Inc.*, 596 F.3d 1343, 1351-52 (Fed. Cir. 2010) (obviousness based on “a single piece of prior art”); *see* Appx28961 (Apple expert report arguing both anticipation and obviousness based on Kiuchi). That would destroy the “finality and repose” issue preclusion is meant to secure. *Del Mar Avionics, Inc. v. Quinton Instrument Co.*, 836



F.2d 1320, 1323 (Fed. Cir. 1987). Apple says it only wants to argue *other* prior art, *see* Apple Brief 58 n.12, but a promise to offer “different evidence” cannot defeat preclusion, *Dana*, 342 F.3d at 1325.

Similar problems attend Apple’s suggestion “that the patents were invalid because they failed to name Dr. Schulzrinne as a co-inventor.” Apple Brief 58 n.12. That non-joinder defense arises under the *same* “statutory section[.]” as anticipation—pre-AIA § 102—and so is precluded even under Apple’s rule. *Id.* at 57. The defense, moreover, essentially rests on an anticipation argument: that a presentation by Dr. Schulzrinne “disclose[d] a number of the inventions allegedly covered by the patents-in-suit.” Appx25428. Because Apple is concededly precluded from rearguing anticipation, its non-joinder defense is likewise foreclosed.

Nor would allowing successive validity challenges by the same party serve the public interest. The “public is best served by getting invalid patents declared invalid as early as possible.” *Hallco Mfg. Co. v. Foster*, 256 F.3d 1290, 1297 (Fed. Cir. 2001). Applying issue preclusion promotes that interest by encouraging defendants to raise all invalidity arguments against a claim at the first opportunity—not hedge their bets across multiple cases, as Apple did here.

**B. Apple Actually Litigated Obviousness and Non-Joinder in the -417 Case**

Apple's efforts to avoid preclusion fail for another, independent reason. Even if different invalidity theories could be "different issues" for preclusion purposes, Apple already litigated—and lost on—obviousness and non-joinder in the -417 case.<sup>6</sup>

Obviousness. Apple took obviousness to trial in the -417 case. *See* Appx25452 (proposed joint pretrial order). It made a last-ditch effort to drop all of its invalidity defenses on the eve of trial, but the district court denied that request *precisely because* such dismissal might not "have the same effect as if we tried it to a jury and the jury returned an adverse finding and the Court entered judgment on the finding adverse to Apple." Appx25487-25490; Appx25591-25592. Invalidity, including obviousness, thus was a live issue at trial. When Apple then "failed to present any evidence" on obviousness defenses it had "announced ready for trial," VirnetX moved for judgment under Rule 50(a). Appx25503-25505; Appx26107-26109. The district court agreed, granting—with Apple's assent—

---

<sup>6</sup> Apple has not identified other invalidity theories it wishes to raise. *See* Apple Brief 58 & n.12; Appx15016-15019. Any such theories are barred. *Kennametal, Inc. v. Ingersoll Cutting Tool Co.*, 780 F.3d 1376, 1385 (Fed. Cir. 2015) ("Arguments not raised until the reply brief are waived." (brackets omitted)).

“judgment as a matter of law on theories of invalidity, other than anticipation over the Kiuchi reference[,] as to the asserted claims.” Appx26113; *see* Appx25523.

That stands in stark contrast to *Voter Verified II*, which held invalidity was “not actually litigated” where the defendant “chose not to respond” to a motion for summary judgment. 887 F.3d at 1383. Apple litigated obviousness all the way to trial, where it suffered an adverse judgment on the merits after failing to carry its burden of proof. When a “‘party who has the burden fails in his proof and the issue is decided against him, he is just as much bound by [issue preclusion] as though he had presented a barrel of testimony.’” *Santopadre v. Pelican Homestead & Sav. Ass’n*, 937 F.2d 268, 274 (5th Cir. 1991). Indeed, judgment as a matter of law under Rule 50(a) is appropriate only where “a party has been fully heard on an issue during a jury trial.” Fed. R. Civ. P. 50(a)(1). By agreeing to (and failing to appeal) judgment under Rule 50(a), Apple conceded the issue was fully litigated.<sup>7</sup>

---

<sup>7</sup> The district court later declined to grant VirnetX judgment on Apple’s invalidity defenses regarding “unasserted claims” not taken to trial. *See* Appx26122-26123 (reserving the issue); Appx22395-22396 (denying VirnetX’s request). Although some language in the court’s order might seem broad enough to cover the *asserted* claims addressed under Rule 50(a), in context nothing suggests the court was reconsidering its earlier decision. It had reserved ruling only on unasserted claims, *see* Appx26122, and Apple opposed judgment only with respect to those claims, *see* Appx25550-25553.

Non-Joinder. Apple also litigated non-joinder in the -417 case. Over Apple's opposition, the district court granted VirnetX partial summary judgment on that defense, finding Apple "lack[ed] sufficient evidence to create a genuine issue of material fact as to whether or not Dr. Schulzrinne conceived the claimed subject matter or contributed to the patented invention." Appx25486. That decision carries preclusive effect. *See Santopadre*, 937 F.2d at 274.

Contrary to Apple's position below, Appx15018, that ruling was not purely procedural. The court did reject Apple's submission of Dr. Schulzrinne's presentation as untimely. But Apple relied on other evidence, including the "deposition testimony of Dr. Schulzrinne and the named inventors," and asserted that "Dr. Schulzrinne offered ample testimony demonstrating that he had previously conceived of the alleged inventions." Appx25422; Appx25428. Apple cannot relitigate the question just because that evidence proved insufficient. *See Dana*, 342 F.3d at 1325.

#### **IV. APPLE IS NOT ENTITLED TO A DECLARATORY JUDGMENT OF NON-INFRINGEMENT AS TO iMESSAGE**

Apple next complains (at 58-61) that the district court denied it a declaratory judgment of non-infringement with respect to iMessage, a feature not addressed at trial. The court's decision was correct. But the issue is moot regardless.

**A. Apple’s iMessage Counterclaim Is Moot**

As explained below, Apple was not entitled to a declaratory judgment of non-infringement. Nonetheless, to eliminate any possible doubt, VirnetX has served Apple with an executed, unconditional, and irrevocable covenant not to sue for direct or indirect infringement of the ’504 and ’211 patents by any version of iMessage in use on or before the date of the covenant, including the iMessage feature in iOS 5-8 and OS X 10.8-10.10. The covenant tracks Apple’s request for declaratory judgment completely, *see* Appx16225, covering past and future sales, offers to sell, and uses of the covered products. *See* Exhibit 1 (attached).

That “unconditional assurance” “enforceably extinguishe[s] any real controversy between the parties” regarding Apple’s iMessage non-infringement counterclaim. *ArcelorMittal v. AK Steel Corp.*, 856 F.3d 1365, 1370-71 (Fed. Cir. 2017); *see Already, LLC v. Nike, Inc.*, 568 U.S. 85, 90-91 (2013). Accordingly, the counterclaim is moot and properly dismissed for lack of jurisdiction. *See PPG Indus., Inc. v. Valspar Sourcing, Inc.*, 679 F. App’x 1002, 1005 (Fed. Cir. 2017); *Apotex Inc. v. Pfizer, Inc.*, 125 F. App’x 987 (Fed. Cir. 2005).

**B. The District Court Properly Declined To Enter Declaratory Judgment**

In any event, the district court properly declined to grant Apple declaratory judgment of non-infringement with respect to iMessage. “The scope of any judgment should conform to the issues that were actually litigated,” taking into account

“what the parties expected to try given their statements and conduct.” *Alcon Research Ltd. v. Barr Labs., Inc.*, 745 F.3d 1180, 1193 (Fed. Cir. 2014). A “formal motion or stipulation” is not necessary “to remove claims from a case” where a party’s words and actions show it is “no longer pursuing” them. *Id.*

Here, VirnetX dropped its infringement claim against iMessage to “narrow[] the case for trial.” Appx89. In response, Apple made clear it would not pursue its non-infringement counterclaim. Just before trial, the district court announced that “one of the accused products, iMessage, has been dropped from the case,” and Apple’s counsel agreed, “That’s right, Your Honor.” Appx1007. Apple’s counsel then affirmed to the court that, “*with the iMessage dropping out*, [30 minutes] should be plenty of time” for opening statements. *Id.* (emphasis added).

Consistent with those representations, at trial “neither party ever put forward any arguments or evidence” regarding iMessage. *Alcon*, 745 F.3d at 1193. Apple never mentioned it in opening or closing—instead telling the jury that the “two groups of two patents” at issue concerned “Facetime” and “VPN On Demand.” Appx2176; *see* Appx2169-2188; Appx2796-2827. Nor did Apple oppose iMessage’s omission from the jury instructions and verdict form. *See* Appx26-52, Appx1154-1177 (delivered instructions and verdict form); Appx26347-26348 (Apple’s proposed verdict form); *contrast* Appx15697 (earlier proposed instructions addressing iMessage). It is inescapable that iMessage was “not

‘litigated, or fairly placed in issue, during the trial.’” *Alcon*, 745 F.3d at 1193. The district court accordingly had “no basis” for entering judgment on it. Appx89.

Apple’s counterarguments are unavailing. Perhaps Apple *could* have insisted that its iMessage counterclaim go to trial despite VirnetX’s decision to drop its claim. *See* Apple Brief 59; *Alcon*, 745 F.3d at 1193. But Apple did not. It affirmed that iMessage had been “dropped from the case,” Appx1007, and proceeded on that basis. It is irrelevant that the iMessage claim and counterclaim were not formally dismissed or struck from the pretrial order. Apple Brief 59-61. A party’s “announcement that it [is] no longer pursuing particular claims, coupled with its ceasing to litigate them, [is] sufficient to remove those claims from the case even without such formalities.” *Alcon*, 745 F.3d at 1193.

For those reasons, the district court properly concluded there was no longer a “substantial controversy . . . of sufficient immediacy and reality to warrant the issuance of a declaratory judgment.” *MedImmune, Inc. v. Genentech, Inc.*, 549 U.S. 118, 127 (2007). When a plaintiff withdraws infringement contentions, “a counterclaimant must show a continuing case or controversy with respect to withdrawn or otherwise unasserted claims.” *Streck, Inc. v. Research & Diag. Sys.*, 665 F.3d 1269, 1283 (Fed. Cir. 2012). Rather than attempt that showing, Apple abandoned its iMessage counterclaim.

Moreover, the Declaratory Judgment Act grants district courts “unique and substantial discretion in deciding whether to declare the rights of litigants” based on “considerations of practicality and wise judicial administration.” *Wilton v. Seven Falls Co.*, 515 U.S. 277, 286, 288 (1995). The district court’s refusal “to penalize or discourage the parties’ efforts in narrowing the case for trial,” Appx89, is precisely the sort of “equitable, prudential, and policy” reason that justifies declining jurisdiction, *MedImmune*, 549 U.S. at 136.<sup>8</sup>

#### **V. APPLE’S REMAINING ARGUMENTS ARE UNAVAILING**

Apple makes several arguments contingent on other cases. It argues (at 61-62) that this Court should vacate the judgment below if VirnetX’s patents are cancelled following other proceedings. That request is premature: Some of those proceedings are still before the PTO, while VirnetX has explained (or will explain) the PTO’s errors in the cases before this Court. Apple also repeats (at 62-68) arguments it concedes are foreclosed by this Court’s summary affirmance in

---

<sup>8</sup> As Apple appears to recognize, the district court’s decision rested on two rationales: “lack of jurisdiction” and “the general policy against discouraging parties from narrowing a case for trial.” Apple Brief 58; *see id.* at 61 (court relied on both “law” and “policy”). It thus can be affirmed on either basis. Where a lower court “dismisses for lack of subject matter jurisdiction and it is clear that the [court] would have declined to exercise its discretionary jurisdiction in any event, [this Court] need not remand.” *Ford Motor Co. v. United States*, 811 F.3d 1371, 1380 (Fed. Cir. 2016).



*VirnetX II*. In the unlikely event of further review in *VirnetX II*, supplemental briefing regarding any implications for this case may be appropriate.

**CONCLUSION**

The judgment should be affirmed.

March 8, 2019

Respectfully submitted,

/s/ Jeffrey A. Lamken

Donald Urrabazo  
URRABAZO LAW, P.C.  
2029 Century Park East  
Suite 1400  
Los Angeles, CA 90067  
(310) 388-9099 (telephone)  
(310) 388-9088 (fax)

*Counsel for Leidos, Inc.*

Jeffrey A. Lamken  
*Counsel of Record*  
Michael G. Pattillo, Jr.  
Lucas M. Walker  
Rayiner I. Hashem  
James A. Barta  
MOLOLAMKEN LLP  
600 New Hampshire Avenue, N.W.  
Washington, D.C. 20037  
(202) 556-2000 (telephone)  
(202) 556-2001 (fax)  
jlamken@mololamken.com

Lauren F. Dayton  
Jennifer E. Fischell  
MOLOLAMKEN LLP  
430 Park Avenue  
New York, NY 10022  
(212) 607-8160 (telephone)  
(646) 710-4945 (fax)

*Counsel for VirnetX Inc.*

Allison M. Gorsuch  
MOLOLAMKEN LLP  
300 North LaSalle Street  
Chicago, IL 60654  
(312) 450-6700 (telephone)  
(312) 450-6701 (fax)

Bradley Wayne Caldwell  
Jason Dodd Cassady  
John Austin Curry  
CALDWELL CASSADY & CURRY  
2101 Cedar Springs Road  
Dallas, TX 75201  
(214) 888-4848 (telephone)  
(214) 888-4849 (fax)

*Counsel for VirnetX Inc.*

# Exhibit 1

### **Covenant Not to Sue**

This Covenant Not to Sue is entered into as of March 1, 2019 (the “**Effective Date**”) by VirnetX Inc. (“VirnetX”), a Delaware corporation.

WHEREAS, VirnetX and Apple Inc. (“Apple”) are parties to an appeal of a patent infringement litigation in the United States Court of Appeals for the Federal Circuit, titled *VirnetX Inc., Leidos, Inc. fka Science Applications International Corporation v. Apple Inc.*, No. 19-1050 (“19-1050 Appeal”); and

WHEREAS, Apple seeks in the 19-1050 Appeal a judgment declaring that its iMessage feature does not infringe certain claims of U.S. Patent Nos. 7,418,504 and 7,921,211;

WHEREAS, VirnetX wishes to resolve any dispute between the parties concerning infringement of U.S. Patent Nos. 7,418,504 and 7,921,211 by Apple’s iMessage feature.

NOW, THEREFORE, VirnetX covenants as follows:

#### **DEFINITIONS**

For purposes of this covenant, the following terms shall have the following meanings:

“**Affiliate**” of a Person means any other Person that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such Person.

“**Device**” means any product supporting iMessage, when configured and operating in a system as specified by Apple, or any product capable of using iMessage, including, but not limited to the Apple iPhone 3GS, iPhone 4, iPhone 4S, iPhone 5, iPhone 5C, iPhone 5S, iPhone 6, and iPhone 6 Plus; Apple iPod Touch devices capable of using iMessage, including the Apple iPod Touch 3rd Generation, iPod Touch 4th Generation, iPod Touch 5th Generation, and iPod Touch with Retina Display; Apple iPad devices capable of using the iMessage functionality, including the Apple iPad, iPad 2, iPad 3rd Generation, iPad 4th Generation, iPad Mini, iPad Mini with Retina Display, iPad Mini 3, iPad Air, and iPad Air 2; Apple computers capable of using iMessage (*e.g.*, running the Messages for Mac application), including Apple computers running OS X 10.7 or higher.

“**Effective Date**” has the meaning set forth in the preamble.

“**Government Authority**” means any federal, state, national, supranational, local, or other government, whether domestic or foreign, including any subdivision, department, agency, instrumentality, authority (including any tax or regulatory authority), commission, board, or bureau thereof, or any court, tribunal, or arbitrator.

“**Asserted Patent[s]**” means U.S. Patent Nos. 7,418,504 (issued on Aug. 26, 2008) and 7,921,211 (issued on April 5, 2011) as they exist on the Effective Date.

“**Person**” means any individual, corporation, partnership, joint venture, limited liability company, Government Authority, unincorporated organization, trust, association, or other entity.

“iMessage” means a messaging service software that uses the Apple Push Notification Service to establish a secure communications link to another iMessage user to send text messages to the recipient that are protected by end-to-end encryption. The term refers to all versions of iMessage existing as of the Effective Date and all versions of iMessage for which Apple has made meaningful preparations to commercialize as of the Effective Date, including, but not limited to, iMessage in iOS 5-8 and OS X 10.8-10.10.

**COVENANT NOT TO SUE**

VirnetX hereby irrevocably covenants that at no time will it, its successors or its assigns, directly or indirectly, alone or by, with, or through others, cause, induce, or authorize, or voluntarily assist, participate, or cooperate in the commencement, maintenance, or prosecution of/commence, maintain, or prosecute any action or proceeding of any kind or nature whatsoever (including, but not limited to, any suit, complaint, grievance, demand, claim, or cause of action in, of, or before any Government Authority) against Apple or any of its Affiliates or any of their past or present directors, officers, employees, successors, assigns, customers, manufacturers, distributors, licensees, or other transferees based upon assertion of direct or indirect patent infringement of any claim of any Asserted Patent by iMessage in any Device.

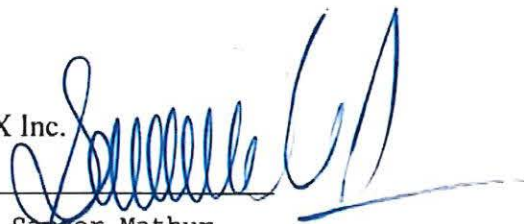
This Covenant Not to Sue shall apply only with respect to the Asserted Patents. It shall not apply with respect to any other patent issued as of the Effective Date or to be issued in the future, including but not limited to (1) patents (including continuation patents) based on the same disclosure as the Asserted Patents, and (2) patents pending but not yet issued as of the Effective Date. This Covenant Not to Sue shall not grant any license, express or implied, with respect to any patent or patent claim other than the claims of the Asserted Patents.

This Covenant Not to Sue shall apply only with respect to iMessage. It shall not apply to any Device with respect to any feature, application, software, service, or product other than iMessage that may infringe any claim of any Asserted Patent or any claim of any other patent. By way of illustration only, this Covenant Not to Sue shall not apply in any way to any aspect of any version of Apple’s FaceTime and VPN on Demand features.

IN WITNESS WHEREOF, VirnetX has executed this Covenant effective as of the Effective Date.

[ATTEST:

Lucas M. Walker  
Witness Name: Lucas M. Walker ]

VirnetX Inc.   
By \_\_\_\_\_  
Name: Sameer Mathur  
Title: Vice President, Corporate Development & Product Marketing

**CERTIFICATE OF SERVICE**

I certify that today, March 8, 2019, I electronically filed the foregoing document with the Clerk of the Court for the U.S. Court of Appeals for the Federal Circuit using the appellate CM/ECF system. Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

March 8, 2019

/s/ Jeffrey A. Lamken

**UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT**  
**CERTIFICATE OF COMPLIANCE MOTIONS OR BRIEFS CONTAINING**  
**MATERIAL SUBJECT TO A PROTECTIVE ORDER**

**Motion / Response / Reply** Containing Material Subject to a Protective Order

- This motion, response, reply complies with the limitations set forth in Fed. Cir. R. 27(m) and contains [*state the number of*] \_\_\_\_\_ words (including numbers) marked as confidential, or
- This motion, response, reply does not comply with the word count limitations set forth in Fed. Cir. R. 27(m) and a motion requesting permission to exceed the maximum word count limitation is being filed contemporaneously with the filing of this motion, response, or reply.
- 

**Briefs** Containing Material Subject to a Protective Order

- This brief complies with the limitations set forth in Fed. Cir. R. 28(d) and contains [*state the number of*] <sup>1</sup> \_\_\_\_\_ words (including numbers) marked as confidential, or
- This brief does not comply with the word count limitations set forth in Fed. Cir. R. 28(d) and a motion is requesting permission to exceed the maximum word count limitation is being filed contemporaneously with the filing of this brief.
- 

\_\_\_\_\_  
/s/ Jeffrey A. Lamken  
(Signature of Attorney)

\_\_\_\_\_  
Jeffrey A. Lamken  
(Name of Attorney)

\_\_\_\_\_  
Appellee  
(State whether representing appellant, appellee, etc.)

\_\_\_\_\_  
March 8, 2019  
(Date)

**CERTIFICATE OF COMPLIANCE**

1. This brief complies with the type-volume limitations of Fed. R. App. P. 32(a)(7)(B) and Fed. Cir. R. 32(a) because this brief contains 13,976 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii) and Fed. Cir. R. 32(b).
2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word in Times New Roman 14-point font.

March 8, 2019

/s/ Jeffrey A. Lamken