

Nos. 26-1317, 26-1355

UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

↔↔↔↔

SPLUNK INC.

Plaintiff-Appellant,

v.

CRIBL, INC.,

Defendant-Cross-Appellant

*On Appeal from the United States District Court
for the Northern District of California, No. C 22-07611 WHA, Judge William Alsup*

DEFENDANT-CROSS-APPELLANT CRIBL, INC.'S PRINCIPAL AND RESPONSE BRIEF

Tigran Guledjian
Christopher Mathews
Valerie Roddy
Amy T. Chau
Sara R. Miller
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
865 South Figueroa St., 10th
Floor
Los Angeles, CA 90017
(213) 443-3000

John F. Bash
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
300 West 6th St., Suite 2010
Austin, TX 78701
(737) 667-6100

William Patry
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
295 5th Ave., 9th Floor
New York, NY 10016
(212) 849-7000

Attorneys for Defendant-Cross-Appellant Cribl, Inc.
July 17, 2026

REPRESENTATIVE PATENT CLAIMS

U.S. Patent No. 9,762,443 – Claim 1

1. A computer-implemented method performed by a remote capture agent coupled to a network, comprising:

obtaining configuration information from a configuration server over a network, wherein the configuration information is usable by the remote capture agent to generate timestamped event data from network packets and to transform the timestamped event data into transformed event data;

monitoring network traffic comprising a plurality of network packets;

generating, based on the configuration information, timestamped event data from at least one network packet of the plurality of network packets, wherein generating the timestamped event data includes segmenting the at least one network packet into a plurality of events and associating each event of the plurality of events with a respective timestamp; and

transforming, based on the same configuration information, the timestamped event data into transformed event data, wherein transforming the timestamped event data includes performing an operation involving data contained in at least one event of the plurality of events.

U.S. Patent No. 10,805,438 – Claim 1

1. A computer-implemented method performed by a configuration server coupled to a remote capture agent via one or more networks, the method comprising:

receiving input requesting creation of an event stream to be generated by the remote capture agent, the input including:

an indication of a protocol to be associated with the event stream, wherein the protocol is used by network traffic monitored by the remote capture agent, and

a selection of an event attribute associated with the protocol, the event attribute indicating data to be extracted from network packets of the network traffic monitored by the remote capture agent;

generating configuration data based on the input; and

sending the configuration data to the remote capture agent, the configuration data causing the remote capture agent to generate the event stream based on the network traffic monitored by the remote capture agent and according to the configuration data.

CERTIFICATE OF INTEREST

Pursuant to Federal Circuit Rule 47.4, undersigned counsel certifies the following:

1. The full names of all entities represented by undersigned counsel in this case: Cribl, Inc.
2. The full names of all real parties in interest for the entities: None/Not Applicable.
3. The full names of all parent corporations and publicly held companies that own 10% or more stock in the entities: None/Not Applicable.
4. The names of all law firms, partners, and associates who have not entered an appearance in this court and (a) appeared for the entity in the lower tribunal, or (b) are expected to appear for the entity in this court: Brian C. Cannon; Joshua Courtney; Scott Alan Florance; Marie M Hayrapetian; Nima Hefazi; Melissa Hurtado; Jordan Kaericher; Evan Kennedy Larson; Jocelyn Ma; Joseph Mel Paunovich; Lana Robins; Scott Schlafer; Margaret H. Shyr; Michael Thomas Zeller.
5. Related cases that meet the criteria under Fed. Cir. R. 47.5(a): None.

6. Information regarding organizational victims and bankruptcy case debtors
and trustees: Not Applicable.

DATED: July 17, 2026

QUINN EMANUEL URQUHART &
SULLIVAN, LLP

By /s/ John F. Bash

John F. Bash

*Attorney for Defendant-Cross-Appellant
Cribl, Inc.*

TABLE OF CONTENTS

	<u>Page</u>
STATEMENT OF RELATED CASES	1
INTRODUCTION	1
STATEMENT OF JURISDICTION.....	6
COUNTERSTATEMENT OF ISSUES PRESENTED.....	6
COUNTERSTATEMENT OF THE CASE.....	7
A. Factual Background.....	7
B. Procedural History.....	12
SUMMARY OF ARGUMENT	16
STANDARDS OF REVIEW	19
ARGUMENT	19
I. RELYING ON THE JURY’S FACTUAL FINDINGS, THE DISTRICT COURT CORRECTLY CONCLUDED THAT CRIBL’S TESTING AND TROUBLESHOOTING WERE FAIR USES	19
A. Cribl’s Testing And Troubleshooting Fall Comfortably Within The Ninth Circuit’s Intermediate-Copying Precedents.....	22
B. The District Court Correctly Applied The Statutory Fair-Use Factors In Light Of The Jury’s Factual Findings	27
II. THE DISTRICT COURT DID NOT ERR IN ITS INTERPRETATION OF THE SGT OR TAP AGREEMENT.....	36
A. The District Court Did Not Err in Its Interpretation of the SGT	38
B. Splunk Forfeited Its Meritless Argument Under The TAP Agreement	42
III. EVEN IF THE DISTRICT COURT ERRED WITH RESPECT TO THE COPYRIGHT OR CONTRACT CLAIMS, THERE ARE NO GROUNDS FOR A NEW TRIAL ON DAMAGES OR A REVISED INJUNCTION.....	48
IV. THE DISTRICT COURT CORRECTLY FOUND THE ’443 AND ’438 PATENTS PATENT-INELIGIBLE UNDER 35 U.S.C. § 101.....	49
A. <i>Alice</i> Step One: The Claims Are Directed to Abstract Ideas	50

1. The District Court Correctly Characterized the Claims at the Appropriate Level of Abstraction50

2. The District Court Correctly Found the Claims Do Not Improve Computer Functionality53

B. *Alice* Step Two: The Claims Recite No Inventive Concept.....57

C. The District Court Did Not Err in Invalidating the Patents on the Pleadings.....61

V. IN THE EVENT THE COURT DISTURBS THE JUDGMENT ON ANY COPYRIGHT ISSUE, CRIBL WAS ENTITLED TO JUDGMENT AS A MATTER OF LAW ON WILLFUL COPYRIGHT INFRINGEMENT64

CONCLUSION71

TABLE OF AUTHORITIES

	<u>Page</u>
 CASES	
<i>Aatrix Software, Inc. v. Green Shades Software, Inc.</i> , 890 F.3d 1354 (Fed. Cir. 2018)	63
<i>Andy Warhol Found. for the Visual Arts, Inc. v. Goldsmith</i> , 598 U.S. 508 (2023).....	27, 28, 30
<i>Atari Games Corp. v. Nintendo of Am., Inc.</i> , 975 F.2d 832 (Fed. Cir. 1992)	40
<i>Bascom Global Internet Servs., Inc. v. AT&T Mobility LLC</i> , 827 F.3d 1341 (Fed. Cir. 2016)	59, 60
<i>Berkheimer v. HP Inc.</i> , 881 F.3d 1360 (Fed. Cir. 2018)	61, 62
<i>Beteiro, LLC v. DraftKings Inc.</i> , 104 F.4th 1350 (Fed. Cir. 2024)	52, 55
<i>Campbell v. Acuff-Rose Music, Inc.</i> , 510 U.S. 569 (1994).....	31, 32, 34, 35
<i>Capitol Recs., LLC v. Escape Media Grp., Inc.</i> , No. 12-CV-06646 AJN SN, 2014 WL 12698683 (S.D.N.Y. May 28, 2014)	66
<i>Carbon Fuel Co. v. United Mine Workers of Am.</i> , 444 U.S. 212 (1979).....	48
<i>Cartoon Network LP, LLLP v. CSC Holdings, Inc.</i> , 536 F.3d 121 (2d Cir. 2008)	65, 66
<i>CDK Glob. LLC v. Brnovich</i> , 16 F.4th 1266 (9th Cir. 2021)	65, 66, 67
<i>Chargepoint, Inc. v. SemaConnect, Inc.</i> , 920 F.3d 759 (Fed. Cir. 2019)	<i>passim</i>

<i>Choate v. Celite Corp.</i> , 215 Cal. App. 4th 1460 (2013)	42
<i>Cisco Sys., Inc. v. Uniloc 2017 LLC</i> , 813 F. App'x 495 (Fed. Cir. May 13, 2020).....	57
<i>De Fontbrune v. Wofsy</i> , 39 F.4th 1214 (9th Cir. 2022)	35
<i>Dr. Seuss Enters., L.P. v. Penguin Books USA, Inc.</i> , 109 F.3d 1394 (9th Cir. 1997)	34
<i>DSC Commc'ns Corp. v. Pulse Commc'ns, Inc.</i> , 170 F.3d 1354 (Fed. Cir. 1999)	25
<i>EEOC v. Go Daddy Software, Inc.</i> , 581 F.3d 951 (9th Cir. 2009)	44, 45
<i>Electric Power Group, LLC v. Alstom S.A.</i> , 830 F.3d 1350 (Fed. Cir. 2016)	60, 61
<i>Ford v. The Silver F, Inc.</i> , 110 Cal. App. 5th 553 (2025)	40
<i>Gardiner, Kamya & Assocs. v. Jackson</i> , 467 F.3d 1348 (Fed. Cir. 2006)	40
<i>Google LLC v. Oracle America, Inc.</i> , 593 U.S. 1 (2021).....	<i>passim</i>
<i>GoTV Streaming, LLC v. Netflix, Inc.</i> , 166 F.4th 1053 (Fed. Cir. 2026)	<i>passim</i>
<i>Harper & Row Publishers, Inc. v. Nation Enters.</i> , 471 U.S. 539 (1985).....	30
<i>Hawk Tech. Sys., LLC v. Castle Retail, LLC</i> , 60 F.4th 1349 (Fed. Cir. 2023)	52, 54
<i>MAI Sys. Corp. v. Peak Comp., Inc.</i> , 991 F.2d 511 (9th Cir. 1993)	66

<i>McGucken v. Pub Ocean Ltd.</i> , 42 F.4th 1149 (9th Cir. 2022)	33, 34
<i>Metro Edison Co. v. N.L.R.B.</i> , 460 U.S. 693 (1983).....	42
<i>Monge v. Maya Magazines, Inc.</i> , 688 F.3d 1164 (9th Cir. 2012)	29
<i>Oracle America, Inc. v. Google Inc.</i> , 750 F.3d 1339 (Fed. Cir. 2014)	8
<i>Packet Intelligence LLC v. NetScout Sys., Inc.</i> , 965 F.3d 1299 (Fed. Cir. 2020)	56
<i>Sanderling Mgmt. Ltd. v. Snap Inc.</i> , 65 F.4th 698 (Fed. Cir. 2023)	59
<i>Sega Enters. Ltd. v. Accolade, Inc.</i> , 977 F.2d 1510 (9th Cir. 1992)	<i>passim</i>
<i>Seltzer v. Green Day, Inc.</i> , 725 F.3d 1170 (9th Cir. 2013)	20
<i>Sony Comput. Ent., Inc. v. Connectix Corp.</i> , 203 F.3d 596 (9th Cir. 2000)	<i>passim</i>
<i>Southern Cal. Gas Co. v. City of Santa Ana</i> , 336 F.3d 885 (9th Cir. 2003)	47
<i>SRI International, Inc. v. Cisco Sys., Inc.</i> , 930 F.3d 1295 (Fed. Cir. 2019)	56, 57
<i>Sutter Home Winery, Inc. v. Vintage Selections, Ltd.</i> , 971 F.2d 401 (9th Cir. 1992)	40, 41
<i>TNS Media Res., LLC v. Tivo Res. & Analytics, Inc.</i> , 629 F. App'x 916 (Fed. Cir. Sept. 16, 2015)	48
<i>Triller Fight Club II LLC v. H3 Podcast</i> , 2023 WL 11877604 (C.D. Cal. Sept. 15, 2023)	30

<i>Trinity Info Media, LLC v. Covalent, Inc.</i> , 72 F.4th 1355 (Fed. Cir. 2023)	58
<i>Two-Way Media Ltd. v. Comcast Cable Commc'ns, LLC</i> , 874 F.3d 1329 (Fed. Cir. 2017)	52
<i>US Patent No. 7,679,637 LLC v. Google LLC</i> , 164 F.4th 1373 (Fed. Cir. 2026)	57, 58

STATUTES

17 U.S.C. § 102	8
17 U.S.C. § 107	<i>passim</i>
28 U.S.C. § 1291	6
28 U.S.C. § 1292	6
35 U.S.C. § 101	<i>passim</i>
Cal. Civ. Code § 1654	40

OTHER AUTHORITIES

Fed. R. Civ. P. 50	44
Splunk, Inc., “Cribl Litigation Update,” <i>available at</i> https://www.splunk.com/en_us/blog/bulletins/cribl-litigation-update.html (last accessed July 17, 2026)	4

STATEMENT OF RELATED CASES

No appeal from this civil action has previously been before this Court or any other appellate court. There is no case pending in this Court or any other court that will directly affect or be directly affected by this Court's decision in this appeal, or that is related to this dispute.

INTRODUCTION

This case is an effort by a software industry incumbent (Splunk) to use patent, copyright, and contract law to prevent an innovative industry newcomer (Cribl) from offering interoperable software that expands customers' freedom of choice over where they send or store their data. Although Splunk and Cribl now offer competing products, the software products at issue in this appeal—Splunk Enterprise and Cribl Stream—are not substitutable.

Splunk Enterprise is a data ecosystem: Splunk “forwarders,” residing on as many as hundreds of thousands of an organization's devices, forward the customer's device data to “indexers” that process the data to permit users to access analytics and insights. Consider, for example, a major bank with a vast network of servers, computers, and ATMs, all of which generate machine data that the bank wishes to analyze, manage, and store or delete.

Cribl Stream is fundamentally different. Customers use Cribl Stream to gather customer data from one or more of multiple data sources, to process that data

midstream, and to send that processed data to multiple destinations for analysis or storage. Cribl Stream's broad interoperability across many different data sources and destinations requires the ability to communicate with data platforms using their specific communication protocols.

At issue here is Cribl's technical copying of object code—solely by execution of software—to discern communication-protocol requirements and ensure interoperability with Splunk Enterprise, which is only one of the many data platforms that Cribl supports. In developing its complementary offering, Cribl did everything right. It pitched its idea for Stream to Splunk before writing a single line of code. Cribl participated in Splunk's partner program and, with Splunk's knowledge, developed Stream's interoperability with Splunk Enterprise by reverse-engineering the essential communication protocol used by Enterprise and continually testing and troubleshooting interoperability to account for updates to Splunk's software. And it launched Cribl Stream in full view of Splunk at Splunk's annual customer conference.

When Splunk eventually grew uncomfortable with Cribl's success, it ripped the rug from underneath Cribl, terminated it as a partner, and filed this lawsuit. In addition to suing Cribl on multiple theories, Splunk sued Cribl's Chief Executive Officer personally and accused Cribl's employees—many of whom were formerly longtime Splunk employees—of taking Splunk's confidential information. The

claims against Cribl's CEO were dismissed by stipulation of the parties; the employees were exonerated at trial.

As to the claims against Cribl, the district court dismissed Splunk's patent-infringement claims on the pleadings for what they were: attempts to dress up unpatentable abstract ideas with the trappings of conventional computers. The copyright and contract claims ultimately proceeded to a jury trial lasting 12 days, generating a 1,946-page transcript, and receiving 118 trial exhibits and live and deposition testimony from 33 fact and expert witnesses.

Both the jury and the district court did yeoman's work to evaluate the highly technical issues in this case and apply settled principles of copyright and contract law. The jury returned a unanimous verdict that found for Cribl on some issues and for Splunk on others, but awarded Splunk only nominal damages because Splunk had failed to prove that any of Cribl's activities had caused it monetary harm given the considerable evidence that Stream had actually *increased* demand for Splunk Enterprise. The district court entered an injunction against Cribl that struck an equitable balance between competing interests, allowing Cribl to run the Splunk

Enterprise software to develop and maintain interoperable software, while enjoining Cribl from making such copies for marketing purposes. Both sides declared victory.¹

Splunk now raises a host of issues on appeal, but none has merit. With respect to the copyright claims, the district court correctly concluded that Cribl’s execution of Splunk Enterprise for reverse-engineering, testing, and troubleshooting was the sort of “intermediate copying” of software that the Ninth Circuit has held to be fair use, because it was designed solely to discover the non-protected functional aspects of Splunk Enterprise to ensure interoperability of the parties’ products. That ruling was supported by the jury findings—unchallenged on appeal—that Cribl’s execution of Splunk Enterprise was necessary for interoperability, was transformative, benefited the public, and caused Splunk no provable loss of revenue.

Splunk essentially asks this Court to construe Ninth Circuit precedent to mean that parties may engage in reverse-engineering of software to *develop* an interoperable product, but may not engage in the testing and troubleshooting necessary to *maintain* the product’s interoperability. That arbitrary distinction conflicts with binding precedent and would, for all practical purposes, nullify fair use for developing interoperable software: No rational actor would develop or adopt

¹ Splunk, Inc., *Cribl Litigation Update*, https://www.splunk.com/en_us/blog/bulletins/cribl-litigation-update.html (last accessed July 17, 2026), *cited at* Appx1586.

interoperable software that a copyright holder could render immediately inoperable by tweaking a single line of code.

Splunk's other appellate arguments are equally misplaced. Splunk has identified no error in the district court's interpretation of the relevant contracts. The plain language of the relevant agreements permitted Cribl to engage in the reverse-engineering, testing, and troubleshooting at issue here. Splunk's contrary interpretations would nullify important provisions of those agreements and violate the principle that any ambiguity should be construed against the drafter—here, Splunk. And the district court's patent-ineligibility dismissal followed directly from this Court's precedents.

For all those reasons, the judgment should be affirmed. But even if this Court were to disagree, there could be no possible ground for Splunk's request for a new damages trial on the copyright and contract claims, because Splunk does not challenge the jury's finding that it is "unknown" if Splunk lost revenue from Cribl's activities—its only claimed damages. Splunk does not address that fatal problem, nor does it justify its request for an injunction under an agreement that Splunk terminated five years ago. Finally, should the Court discern any reversible error with respect to the copyright claims, the Court should also reverse the district court's denial of Cribl's motion for judgment as a matter of law with respect to willful copyright infringement.

The Court should affirm the judgment.

STATEMENT OF JURISDICTION

Cribl does not dispute Splunk's Statement of Jurisdiction. Br. 5. With respect to Cribl's cross-appeal, on December 31, 2025, the district court denied Cribl's timely motion for renewed judgment as a matter of law. Appx50-76. After Splunk filed its notice of appeal the same day, Cribl filed a timely notice of cross-appeal. Appx1653-1656. This Court has jurisdiction over Cribl's cross-appeal under 28 U.S.C. §§ 1291 and 1292(c)(2).

COUNTERSTATEMENT OF ISSUES PRESENTED

Appeal:

1. Whether the district court committed reversible error in finding that any unlicensed, incidental copying of Splunk's copyrighted object code arising from Cribl's downloading and execution of Splunk Enterprise for purposes of testing and troubleshooting to maintain interoperability with Cribl Stream was a fair use under Section 107 of the Copyright Act.
2. Whether the district court correctly interpreted provisions of the parties' agreements to allow for the fair use of Splunk Enterprise software, including through reverse-engineering, testing, and troubleshooting.
3. Whether there is any basis to remand for a new trial or revisit the scope of the injunction.

4. Whether the asserted claims of U.S. Patent Nos. 9,762,443 and 10,805,438 are patent-ineligible under 35 U.S.C. § 101.

Conditional Cross-Appeal:

5. Only to the extent this Court disturbs any copyright aspect of the judgment or injunction below, whether the district court erred in denying Cribl’s renewed motion for judgment as a matter of law as to willful copyright infringement.

COUNTERSTATEMENT OF THE CASE

A. Factual Background

1. Founded in 2003, Splunk licenses and distributes Splunk Enterprise, software for organizations that ingests and analyzes machine data. Appx51. A business installs Splunk “forwarders” at its data sources. *Id.* The forwarders then send the customer’s data to a Splunk “indexer” for ingestion into Splunk Enterprise, which allows users to gain insights into their data. *Id.*

The Splunk forwarding process uses a communication format known as the S2S (“Splunk-to-Splunk”) protocol. Appx2; Appx2798. A protocol is a set of rules governing how software programs communicate with one another—a shared format that allows one program to send data and instructions to another in a form the receiving program can understand. Appx2. S2S is one such protocol, defining the format in which data travels from Splunk forwarders to Splunk indexers. *Id.* Importantly, a protocol is a prescribed format for communicating data; it is not itself

software. Appx52. For that reason, it is undisputed that the S2S protocol is not copyrightable. *Id.*; see *Oracle America, Inc. v. Google Inc.*, 750 F.3d 1339, 1354 (Fed. Cir. 2014) (“Copyright protection extends only to the expression of an idea—not to the underlying idea itself.”); 17 U.S.C. § 102(b).

Splunk distributes Splunk Enterprise under its Splunk General Terms license (“SGT”). Its “General Rights” provision grants users the right to use offerings for their own “Internal Business Purposes,” and its restrictions are framed expressly as “Use Restrictions.” Appx4169 (SGT § 1(A)); Appx4172 (SGT § 9). As particularly relevant here, the SGT allows reverse-engineering “to the extent specifically permitted by statutory law.” Appx4172 (SGT § 9(a)).

2. In 2017, three Splunk employees—Clint Sharp, Ledion Bitincka, and Dritan Bitincka—left Splunk to start their own venture. Appx51. They sought to create a vendor-agnostic tool that would provide customers control over their data while enabling them to optimize, filter, and enrich their data in real time—what is now widely known as “stream processing.” Appx3299-3300; Appx3327-3329. That idea ultimately became Cribl Stream.

From the outset, Cribl was open with Splunk about its planned product launch. In June 2018, Sharp emailed Splunk employees about Cribl’s idea for what would become Cribl Stream. Appx5445. A Splunk employee replied that he was “excited because [Cribl’s idea] line[d] up pretty damn close with one of [Splunk’s]

customer's actual needs right now." Appx5444. The following month, the same Splunk employee emailed a Splunk customer attaching Cribl's pitch deck and affirmatively marketing Cribl—before Cribl had written its first line of code. Appx3323-3324; Appx5433-5435.

Cribl's Sharp went on to share his plan for Cribl across the Splunk organization, including with Rick Fitz, Splunk's Senior Vice President of IT Markets and a direct report of Splunk's Chief Executive Officer, who forwarded Sharp's pitch to Splunk's Vice President of Product Management and other senior engineering leadership. Appx5439-5440. Fitz's email described Cribl as trying to "build something that all Splunk customers would want" and seeking "the broad support of Splunk before spending a lot of energy." *Id.*; Appx3325-3326.

Cribl designed Stream to communicate with multiple data sources and destinations—more than 70 at the time of trial—through numerous communication protocols, allowing it to interoperate with many data platforms, not just Splunk Enterprise. Appx2814. For that reason, Splunk's repeated suggestion that Cribl somehow operates "within" Enterprise, as though it is embedded in Splunk's software, is not accurate. Stream operates on data as it travels from sources to destinations, which include Splunk forwarders and indexers but also many other data platforms. Appx2.

But for Enterprise users who wished to send the data gathered by Splunk's forwarders to Cribl Stream for midstream processing, it was critically important for end-users that Cribl Stream be interoperable with Splunk Enterprise using the S2S protocol because adherence to that protocol was the only way for users to receive complete and unaltered data from Splunk's forwarders. Appx2807-2808; Appx2813; Appx40-41 (Phase One Verdict Form Nos. 1, 2, 4). Cribl was therefore required to develop its own implementation of the S2S protocol. Appx2807-2808; Appx53.

Ledion Bitincka wrote Cribl's first S2S protocol Stream integration himself. Appx2807. To understand the protocol, he launched two instances of Splunk Enterprise, configured each to communicate with the other using the S2S protocol, and monitored the network traffic between them to understand the protocol. Appx2810-2813. Both parties' expert witnesses later confirmed that such network-traffic analysis is a standard industry technique. *See, e.g.*, Appx3514-3515 (Cribl's expert testifying network-traffic analysis is commonly used across industry); Appx3058-3060 (Splunk's expert testifying Splunk itself used packet-sniffing techniques to understand communications from Cribl's software).

By October 2018, Cribl had developed as part of Stream its own Splunk Enterprise integration using its reverse-engineered version of the S2S protocol. Appx2808. Cribl was again transparent with Splunk about its S2S implementation. In September 2018, Bitincka asked senior Splunk engineer Mitchell Blank for

troubleshooting help with Cribl's S2S integration. Appx2845-2850. No Splunk employee ever told Cribl it was not allowed to communicate with Splunk software using the S2S protocol, that it needed Splunk's permission to do so, or that it needed a special license to build such an integration. Appx2850-2852. And, although it was aware of Cribl Stream's interoperability with Splunk Enterprise, Splunk never accused Cribl of breaching any provision of the SGT (until it filed this lawsuit). Appx3355.

3. In August 2018, Splunk accepted Cribl into its Technology Alliance Partner ("TAP") Program. Appx51. Splunk designed the TAP Program to grow its "partner ecosystem" and promote the development of complementary technology solutions extending Splunk Enterprise's features and functionality. Appx5353. The TAP Agreement, governing participation in the TAP program, granted Cribl a license to use Splunk Enterprise to develop, test, and market applications that extended the features and functionality of Splunk software, including to "support interoperability between the Splunk Software and [Cribl's] system." Appx5109-5110 (TAP § 3.3(i)); Appx67.

Being in the TAP program allowed Cribl to attend Splunk's annual user conference, which was the fastest way to reach a large concentration of Splunk customers. Appx3330-3331; Appx3334-3335. At the October 2018 conference, Cribl publicly debuted Cribl Stream and demonstrated its interoperability with

Enterprise. Appx3335-3337. From at least that point forward, Splunk was fully aware that Cribl Stream used an S2S integration to communicate with Enterprise. Appx2845-2852; Appx3334-3337. At all times during Cribl's TAP partnership, Cribl was also licensed to use Splunk Enterprise under the SGT, the same license available to ordinary users. Appx51.

Even as the TAP partnership continued, Splunk was developing its own stream processing product, Splunk Data Stream Processor, to compete with Cribl Stream. Appx62. For more than a year, Splunk planned to terminate Cribl as a partner as soon as it could offer a viable alternative to Stream. Appx17. Unaware of Splunk's intentions, Cribl continued investing in Cribl Stream. *Id.* In November 2021, Splunk terminated Cribl from the TAP program. Appx52.

B. Procedural History

1. In December 2022, Splunk sued Cribl in the United States District Court of the Northern District of California, asserting claims for copyright infringement, breach of the SGT and TAP Agreement, and patent infringement, as well as other claims not relevant here. Appx319-403.

Splunk asserted two copyright claims at trial. *First*, Splunk alleged that Cribl infringed Splunk's copyrighted source code when a Splunk employee, later hired by Cribl, inadvertently copied a Splunk source code repository (a claim that ultimately hinged on agency issues). Appx388-395. *Second*, Splunk alleged that Cribl infringed

Splunk’s copyrighted object code by making unlicensed copies of Splunk’s copyrighted object code every time it executes Splunk Enterprise in connection with the development of its software. *Id.* Cribl raised fair use under Section 107 of the Copyright Act, 17 U.S.C. § 107, as an affirmative defense, alleging that its use of Splunk Enterprise to reverse-engineer the S2S protocol, as well as for testing, troubleshooting, and customer demonstrations of Cribl Stream, fall within the scope of that doctrine and therefore did not give rise to liability. Appx791-792.

Splunk’s breach-of-contract claim alleged that Cribl violated Section 9 of the SGT and Section 4 of the TAP Agreement by reverse-engineering Splunk Enterprise software to determine source code, algorithms, methods, or techniques embodied in that software and by developing Cribl Stream. Appx395-396. Splunk further alleged that Cribl violated Section 9 of the SGT by using trial and commercial versions of Splunk Enterprise for competitive purposes, such as developing, testing, and marketing its own software. Appx396-398.

2. Cribl moved to dismiss the patent-infringement claims under Section 101 of the Patent Act, 35 U.S.C. § 101. Appx404-435. The district court granted the motion. Appx77-106. The court determined the representative claims were not patentable under *Alice* step one because they “merely invoke generic processes and machinery” and “do not offer specific technical solutions to specific technical

problems,” Appx94-95, and that at *Alice* step two they disclosed nothing inventive. Appx91-101.

3. The case proceeded to trial. After the presentation of evidence, the district court divided the jury’s deliberations into two phases. Appx52.

In phase one, the jury resolved underlying factual questions bearing on Cribl’s fair-use defense to the copyright claims. *Id.* The jury returned a unanimous special verdict finding that (i) Cribl could not viably interoperate with Splunk forwarders and indexers without reverse-engineering the S2S protocol; (ii) reverse-engineering was the only means of determining that protocol; (iii) other protocols Splunk claimed Cribl could have used were not viable alternatives to the S2S protocol for interoperability; (iv) whether Splunk would have earned more money but for Cribl’s copying was unknown; (v) the public benefited from Cribl’s copying and use of Splunk Enterprise; and (vi) Cribl’s S2S protocol capability was a transformative use. Appx40-42 (Phase One Verdict Form Nos. 1-7).

Based on those findings, the district court then concluded that Cribl’s copying of Splunk Enterprise for reverse-engineering, testing, and troubleshooting was fair use under Section 107, but that its customer demonstrations (what the court called “marketing”) was not. Appx8-9.

In phase two, the district court informed the jury about its fair-use conclusion and instructed the jury on the substantive elements of Splunk’s claims. Appx3948-

3961. Following further deliberations, the jury returned a unanimous verdict finding for Splunk on certain claims but awarding only \$1 in nominal damages, consistent with its phase one finding that it was “unknown” whether Splunk had lost any revenue on account of Cribl’s activities. Appx43-46 (Phase Two Verdict Form); Appx41 (Phase One Verdict Form).

With respect to Splunk’s copyright claims, the jury found for Cribl on the claim alleging copying of source code. Appx43 (Phase Two Verdict Form No. 1A). The jury found, however, that Cribl had willfully infringed Splunk’s copyright in its object code when it downloaded and executed the Enterprise software. Appx44 (Phase Two Verdict Form Nos. 1B, 2).

As to Splunk’s breach-of-contract claims, the jury found that Cribl had not breached the TAP Agreement, but that it had breached the SGT. Appx44 (Phase Two Verdict Form Nos. 4, 5). The verdict did not specify which activities breached the SGT. *Id.*

The district court granted Splunk’s motion for a permanent injunction barring Cribl from using Splunk Enterprise for marketing purposes, but the court permitted Cribl to continue using Splunk Enterprise for all fair uses under the Copyright Act, including reverse-engineering, testing, and troubleshooting for interoperability. Appx47-49. The court acknowledged that a sensible reading of the jury’s verdicts was that it found Cribl breached the SGT by marketing alone, but also found that,

even if it assumed the jury found reverse engineering, testing, and troubleshooting also breached the SGT, the balance of equities and the public interest warranted enjoining only Cribl's use of Splunk Enterprise for marketing activities. Appx14-18. The court denied all other post-judgment motions, including Cribl's motions for judgment as a matter of law on willful copyright infringement and the enforceability of the SGT. Appx76.

SUMMARY OF ARGUMENT

This Court should affirm the judgment in full. But should the Court disturb the judgment with respect to either liability or remedies on the copyright or contract claims, it should reverse the district court's denial of Cribl's motions for judgment as a matter of law on willful copyright infringement.

I. Copyright Claims. The district court correctly entered judgment for Cribl on its fair-use defense with respect to its copying of Splunk Enterprise (*i.e.*, running downloaded instances) to reverse-engineer the S2S protocol needed to make Cribl's Stream interoperable with Enterprise and to troubleshoot and test Cribl Stream's interoperability with Enterprise. That conclusion was well supported by the jury's factual findings—unchallenged on appeal—that Cribl's uses of Splunk Enterprise were transformative and had not been shown to cause Splunk any losses.

Although Splunk does not dispute that reverse-engineering the S2S protocol to achieve Stream's interoperability with Splunk Enterprise was fair use, it claims

that the testing and troubleshooting necessary to *maintain* interoperability was not. That arbitrary distinction rests on a misunderstanding of the relevant Ninth Circuit precedents. The district court correctly concluded that testing and troubleshooting fall well within the scope of permissible “intermediate copying” under those controlling decisions. Splunk’s other arguments largely depend on the same misreading of precedent and at any rate lack merit.

II. Breach-of-Contract Claims. Splunk takes issue with the district court’s interpretation of the SGT and the TAP Agreement to permit certain fair uses of Splunk Enterprise. The district court’s interpretation of the provisions at issue properly give effect to their plain language and read their various provisions harmoniously. To the extent the licenses are ambiguous, the district court correctly construed them against Splunk as the drafter.

III. Injunction and Damages. Splunk’s arguments in favor of a new trial and injunction are admittedly derivative of its merits arguments on the copyright and contract claims and fail for the same reasons. But at any rate, because Splunk does not challenge the jury’s unanimous factual finding that it is unknown if Cribl’s actions caused Splunk any injury, a new trial on damages would not be warranted. Splunk’s request for an injunction enforcing the TAP Agreement, moreover, is moot because that agreement was terminated in 2021. Further, even if Splunk could show error in the district court’s interpretation of the SGT, the district court assumed the

broadest possible liability in fashioning the injunction in this case and drew it narrowly because of the balance of hardships and public interest, not on the basis of the contractual interpretations Splunk challenges on appeal.

IV. Patent Claims. The district court correctly dismissed Splunk’s patent claims as asserting patent-ineligible, invalid patents. The two patents that Splunk raises on appeal are prototypical examples of software-related patents asserting claimed methods that do nothing more than describe an abstract idea (generating and transforming data) using ordinary computer functions, with no inventive step. They accordingly fall squarely within this Court’s decision in *Chargepoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759 (Fed. Cir. 2019), which held invalid under Section 101 patents relating to a communication network that—like those here—claimed neither a technical improvement nor a means of overcoming a technical difficulty.

V. Conditional Cross-Appeal: If the Court finds reversible error in the judgment or injunction with respect to the copyright claims, it should reverse the district court’s denial of Cribl’s motion for judgment as a matter of law. Splunk failed to present substantial evidence that Cribl knew or willfully disregarded the risk its marketing activities were unauthorized or infringing, and it failed to present *any* evidence of the duration Splunk’s code stayed in RAM, a required element of Splunk’s claim.

STANDARDS OF REVIEW

Although Splunk’s statement of the standards of review is largely correct, Br. 27, its description of the standard of review for a fair-use determination is incomplete. Because fair use is “a mixed question of fact and law,” “reviewing courts should appropriately defer to the jury’s findings of underlying facts,” although the “ultimate question whether those facts show[] a ‘fair use’ is a legal question for judges to decide *de novo*.” *Google LLC v. Oracle America, Inc.*, 593 U.S. 1, 23-24 (2021). Thus, a court must review for substantial evidence the jury’s resolution as to “subsidiary factual questions, such as ‘whether there was harm to the actual or potential markets for the copyrighted work.’” *Id.* at 24 (citations omitted).

ARGUMENT

I. RELYING ON THE JURY’S FACTUAL FINDINGS, THE DISTRICT COURT CORRECTLY CONCLUDED THAT CRIBL’S TESTING AND TROUBLESHOOTING WERE FAIR USES

The district court correctly concluded, consistent with the jury’s findings, that Cribl’s copying of Splunk Enterprise to reverse-engineer the uncopyrightable S2S protocol and to test and troubleshoot Cribl Stream’s interoperability with Splunk Enterprise was fair use under Section 107 of the Copyright Act. Appx1-9.

Section 107 provides that “the fair use of a copyrighted work . . . is not an infringement of copyright.” 17 U.S.C. § 107. Courts evaluating a fair-use defense must consider “(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of

the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.” *Id.*

Two features of Ninth Circuit precedent have particular relevance here. First, genuine questions of “historical fact[]” pertaining to the fair-use determination must be resolved by the jury, *Seltzer v. Green Day, Inc.*, 725 F.3d 1170, 1175 (9th Cir. 2013), and the jury’s findings may be disregarded only for lack of substantial evidence, *Google*, 593 U.S. at 23-25. Thus, questions like whether the defendant’s use was transformative and whether the copying caused harm to the actual or potential market for the copyrighted work are properly resolved by juries.

Second, the Ninth Circuit has held that so-called “intermediate copying” can qualify as fair use. *See Sony Comput. Ent., Inc. v. Connectix Corp.*, 203 F.3d 596, 602-03, 605-06 (9th Cir. 2000); *Sega Enters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1518-19, 1525-27 (9th Cir. 1992). Intermediate copying refers to copying a copyrighted computer program not to exploit its expression, but as a necessary step to gain access to the program’s uncopyrightable functional elements, such as interfaces, protocols, or other rules needed for interoperability. *See id.* In *Sega* and *Sony*, the Ninth Circuit held that, where intermediate copying is the only way to reach functional elements and there is a legitimate reason for seeking them, copying and “disassembly [are] fair use of the copyrighted work, as a matter of law,” even

though the defendant necessarily makes complete copies of the copyrighted program in the process. *Id.* at 1527-28.

Faithfully applying these principles, the district court first asked the jury to resolve a number of factual questions relevant to whether Cribl's copying of Splunk Enterprise was permissible fair use. The jury found, among other things, that Cribl could not viably interoperate with Splunk forwarders and indexers without reverse-engineering the S2S protocol, that the public benefited from Cribl's copying and use of Splunk Enterprise, and that Cribl's S2S capability was a transformative use. Appx40-42. The jury also found it was "unknown" if Splunk would have earned more money but for Cribl's copying. *Id.*

Based on those factual determinations and applying the statutory factors, the district court held that this was a case of justified intermediate copying. Appx7. The court explained that "the entire Splunk Enterprise software program was by necessity downloaded and run for reverse-engineering the uncopyrighted S2S protocol and viably interoperating Cribl Stream with Splunk Enterprise." Appx7. Cribl made intermediate copies of Splunk Enterprise not to incorporate it into Cribl Stream—indeed, Cribl copied Splunk's object code, which is in a binary form that cannot be read by humans or incorporated into a product—or distribute it to customers. Rather, Cribl needed to understand the uncopyrightable S2S protocol

embedded in the software to enable Cribl Stream to interoperate (and continue to interoperate) with Splunk forwarders and indexers.

In challenging that ruling on appeal, Splunk essentially ignores the jury’s factual findings, and it accepts the district court’s conclusion that copying to *reverse-engineer* the S2S protocol was a fair use. But it claims that the district court erred as a matter of law in finding that copying to *test and troubleshoot* Cribl’s software embodying the S2S protocol—*i.e.*, running Splunk Enterprise to ensure that, as the software is updated, it continues to interoperate with Cribl Stream—is also fair use. That position that would render the initial reverse-engineering all but pointless. Splunk’s argument—which focuses on quantity and frequency instead of nature and purpose—rests largely on a misunderstanding of the Ninth Circuit’s precedents on “intermediate copying.” The Court should accordingly affirm the district court’s fair-use ruling.

A. Cribl’s Testing And Troubleshooting Fall Comfortably Within The Ninth Circuit’s Intermediate-Copying Precedents

Splunk’s principal argument on appeal is that Cribl’s copying of Splunk Enterprise for troubleshooting and testing does not qualify as intermediate copying because it was “pervasive, constant, and ongoing” and involved “Cribl’s maintenance of a competitive product that operates in between Splunk’s software.” Br. 27-30 (emphasis omitted). Neither contention has merit.

1. With respect to the first claim, both of the Ninth Circuit’s key precedents involved copying that was materially similar to the copying here. For example, although Splunk claims *Sega* involved “one-time reverse-engineering,” Br. 29, that characterization obscures what actually happened in the case. In *Sega*, a video-game maker needed “to render its video games compatible with [Sega’s] Genesis console.” 977 F.2d at 1514. To do so, it engaged in an iterative, experimental process: After initially disassembling the object code contained in Sega game cartridges into source code, the defendant’s engineers “loaded the disassembled code back into a computer, and experimented to discover the interface specifications for the Genesis console by modifying the programs and studying the results.” *Id.* at 1514-15.

That process used to ensure compatibility is akin to what happened here. To build an interface for Cribl Stream to make it interoperable, *i.e.*, compatible, with Splunk’s Enterprise software, Cribl engaged in an iterative, experimental process. It ran two copies of Enterprise, set them up to communicate with each other, and reverse-engineered a working version of the S2S protocol by studying the communications between them. But in order for that work to remain effective, Cribl was required to run Splunk Enterprise to detect and address updates to Enterprise—the testing and troubleshooting that Splunk claims falls outside of the ambit of fair use.

There is no material difference between that activity and what was approved in *Sega*. Nothing in *Sega* suggests that intermediate copying ceases to be fair use simply because maintaining interoperability requires additional rounds of reverse-engineering or testing. Rather, *Sega*'s rule turns on the purpose of the copying—whether it is necessary to discover uncopyrightable functional elements needed for interoperability—not on the number of times the copying occurs. Tellingly, Splunk's revisionist take on the opinion—that it turned on “copying on a one-time, temporary basis”—never actually quotes any passage of the opinion supporting Splunk's rule. Br. 28.

Sony was similar. In that case, Connectix sought to build a software program that would allow users to play games originally designed for the Sony PlayStation on a personal computer. 203 F.3d at 598. To do so, Connectix “*repeatedly* copied Sony's copyrighted [software program that operated the PlayStation].” *Id.* (emphasis added). As the Ninth Circuit explained, the defendant “made daily copies” of that software, “repeatedly copied and disassembled discrete portions” of the software to debug its own emulation software, and used the software throughout development of both its Macintosh and Windows versions. *Id.* at 601. The *Sony* court specifically rejected the argument that those repeated copies were unnecessary because Connectix could have chosen an engineering path involving less copying, holding that the relevant inquiry was “the necessity of the method, i.e., disassembly, not the

necessity of the number of times that method was applied.” *Id.* at 605. Here, Splunk essentially ignores *Sony*’s holding and reasoning, claiming that the fact that Cribl’s copying, *i.e.*, running of Enterprise, was “daily” means it does not qualify as “intermediate copying,” Br. 28, even though the same was true in *Sony*.

Controlling precedent aside, Splunk’s argument makes little practical sense. Splunk essentially contends that the fair-use doctrine may protect the first round of reverse-engineering to *establish* interoperability, but not the subsequent testing and troubleshooting required to *maintain* interoperability. That ignores the practical realities of software engineering. Splunk’s software is a moving target; Splunk distributes Splunk Enterprise in updated versions on a continuing basis, and the S2S protocol is implemented in that software. *See, e.g.*, Appx58 (district court noting Splunk’s “herkie-jerky changes” to Enterprise) (citing Appx5663). When Splunk releases a new version of Enterprise, Cribl’s engineers must check to ensure its Stream software remains interoperable with Enterprise’s S2S protocol so that Cribl Stream continues to receive data correctly from Splunk forwarders. As the district court recognized, “copying and using Splunk Enterprise to reverse engineer the S2S protocol, as required to viably interoperate Cribl Stream with Splunk Enterprise, accomplishes nothing if Cribl cannot copy and use Splunk Enterprise to test and troubleshoot Cribl Stream for maintaining the interoperability.” Appx74-75. That purpose stands in marked contrast to the copying in *DSC Communications Corp. v.*

Pulse Communications, Inc., 170 F.3d 1354 (Fed. Cir. 1999) (cited in *Splunk Br. 30*), the only purpose of which was to aid the commercial deployment of a finished product, not to ensure continued interoperability.

At base, *Splunk* misconceives the purpose of the intermediate-copying doctrine. The doctrine’s fundamental insight is that copyright should not be used to prevent competitors from discovering and replicating the non-copyrightable aspects of computer programs. As *Sony* put it, “the Copyright Act protects expression only, not ideas or the functional aspects of a software program,” and “the fair use doctrine preserves public access to the ideas and functional elements embedded in copyrighted computer software programs.” 203 F.3d at 603. But if the law prevented software developers from testing and troubleshooting the functional elements of a program to maintain interoperability, it would have the practical effect of blocking public access to those elements. For that reason, there is no principled distinction between the initial reverse-engineering required to establish interoperability, and testing and troubleshooting required to maintain that interoperability.

2. *Splunk* never explains its assertion that the intermediate-copying doctrine does not apply here because *Stream* “operates in between *Splunk*’s software,” *Br. 28*, other than to claim that “*Cribl*’s copying . . . does not give rise to any new ‘creative expression,’” *Br. 30* (quoting *Sega*, 977 F.2d at 1523). That is clearly incorrect. *Cribl* used the functional elements of *Splunk Enterprise* to ensure that its

own software—indisputably a form of creative expression—can interoperate with the Enterprise platform. That is no different from *Sony*, where Connectix ensured that existing games produced by other parties for the PlayStation would work with its new software.

B. The District Court Correctly Applied The Statutory Fair-Use Factors In Light Of The Jury’s Factual Findings

The district court correctly concluded that, in light of the jury’s findings (unchallenged on appeal), three of the four statutory fair-use factors favored fair use. Appx4-8. Splunk’s contrary arguments lack merit.

Factor 1. The first fair-use factor considers whether the copying had a further purpose or different character from the original work. *Andy Warhol Found. for the Visual Arts, Inc. v. Goldsmith*, 598 U.S. 508, 525 (2023). As discussed above, the district court correctly found that Cribl “copied and used copyrighted software to gain access to the functional elements of that software”—the uncopyrightable S2S protocol—and then built an interoperable product. Appx5. That is a different purpose and character from Splunk Enterprise, which is a data ecosystem designed for ingestion, analysis, and monitoring. That alone weighs in favor of a fair-use determination. Splunk raises a handful of arguments under the first factor, but they largely conflict with the controlling Ninth Circuit decisions in *Sega* and *Sony*.

First, Splunk argues that “Cribl’s software ‘share[s] substantially the same purpose’ as the original work,” because Cribl Stream operates in the same data

environment as Splunk Enterprise and both products capture, index, route, and analyze data. Br. 31-32 (quoting *Warhol*, 598 U.S. at 526). But that argument erroneously focuses on the general purpose of *Cribl Stream* rather than *the challenged use of Splunk Enterprise*. The relevant question is why Cribl copied and used Splunk Enterprise for testing and troubleshooting—not whether Cribl Stream and Splunk Enterprise perform some overlapping functions. Indeed, Splunk does not contend Cribl Stream contains *any* of Splunk Enterprise’s code. Thus, as the district court concluded, Cribl’s copies of Splunk Enterprise “were not made to duplicate and supplant the copyrighted software”; they were made to access the uncopyrightable S2S protocol and achieve interoperability. Appx5.

Splunk tries to draw a parallel to the Supreme Court’s recent *Warhol* decision, but there it was the copying itself that had a similar purpose to the original work. In *Warhol*, the infringer commercially licensed an artistic silkscreen portrait of Prince derived from a copyrighted photograph for use on the cover of a magazine—the same market in which the original photograph had itself been licensed for substantially the same purpose. *Warhol*, 598 U.S. at 525-28, 534-36. At any rate, even if the purpose of Cribl Stream were relevant here, Splunk’s argument is wrong on its own terms. While both Stream and Enterprise work within the same customer “data environment” as a general matter, Stream allows customers to communicate with more than 70 data sources and destinations far beyond Enterprise, using

numerous communication protocols other than S2S. Appx2814. The purpose and function of the two products are fundamentally distinct.

Second, Splunk argues that testing and troubleshooting were not transformative because Cribl copied and ran the entirety of Splunk Enterprise. Br. 32-33. But that argument has nothing to do with the purpose of the use, and it runs headlong into *Sega* and *Sony*, both of which permitted the full copying of software for intermediate copying. *Sony*, 203 F.3d at 606; *Sega*, 977 F.2d at 1522-23.

Third, Splunk argues that “Cribl’s copying was overwhelmingly commercial.” Br. 33. But although commerciality is relevant, *Sega* held that the commercial nature of intermediate copying carries little weight because the commercial exploitation is only “indirect or derivative.” 977 F.2d at 1522; *see Sony*, 203 F.3d at 606-07. Further, here, the jury’s finding that the public benefited from Cribl’s copying and use of Splunk Enterprise, Appx41, favors fair use “notwithstanding the fact that the alleged infringer may gain commercially.” *Sega*, 977 F.2d at 1523.

Finally, citing dicta in a footnote in a Ninth Circuit decision, Splunk argues that the district erroneously ignored Cribl’s supposed subjective bad faith. Br. 34-35 (citing *Monge v. Maya Magazines, Inc.*, 688 F.3d 1164, 1173 n.6 (9th Cir. 2012)). But the court’s analysis made clear that Cribl’s subjective purpose was “to reverse engineer the S2S protocol used by the copyrighted software—which was itself

unprotected and uncopyrightable—and to interoperate with the copyrighted software.” Appx5. That is not the sort of subjective bad faith that Splunk’s cases deem to disfavor fair use; nor is a simple breach of contract. *See Triller Fight Club II LLC v. H3 Podcast*, 2023 WL 11877604, at *2, 8-9 (C.D. Cal. Sept. 15, 2023) (bootlegging copyrighted broadcast of boxing match); *see also Harper & Row Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 562-63 (1985) (discussing bad faith of magazine that “scoop[ed]” authorized publishers using “purloined” manuscript). Here, the district court found that it was in fact *Splunk* that had acted in bad faith with respect to Cribl’s use of Splunk’s copyrighted software: “[T]his was not a case of a copyright pirate selling knockoffs. This was a case of a ‘partner’ being invited in by a copyright owner to use the copyrighted work, and to invest millions in designing and developing a complementary product, only to be terminated after all that effort was made.” Appx17.

At any rate, the district court correctly recognized that recent Supreme Court decisions have explained that “fair use is an objective inquiry into what a user does with an original work, not an inquiry into the subjective intent of the user,” casting doubt on contrary statements in lower-court decisions. *Warhol*, 598 U.S. at 545; *see Google*, 593 U.S. at 32-33. Splunk is incorrect (Br. 35-36) in claiming that those statements were limited the transformativeness component of the first factor.

Factor 2. The second fair-use factor considers the nature of the copyrighted work, recognizing that some works are “closer to the core of intended copyright protection than others,” *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 586 (1994), and that where “copyrightable material is bound up with uncopyrightable material, copyright protection is ‘thin.’” *Google*, 593 U.S. at 21. The district court correctly found this factor favors Cribl on two independent grounds.

First, the district court focused on the actual code copied, as the Supreme Court’s decision in *Google* requires. 593 U.S. at 27-29. The court explained that “it was the executable object code that was copied” by downloading and executing Splunk Enterprise, and “no evidence compelled the conclusion that creativity in the source code . . . ever propagated into the object code.” Appx60. Splunk claims (Br. 41-42) that any creativity in the source code necessarily carried over to the object code, but it cites scant record evidence for that claim, relying largely on the undisputed proposition that copyright protection can extend to object code. It has shown no error in the district court’s finding that the record lacked sufficient support for Splunk’s assertion. Attorney assertions in an appellate brief cannot make up for the lack of record evidence that the district court found.

Second, the district court found that “no evidence compelled the conclusion that [unprotected] functional elements could have been copied separately from creative elements.” Appx60. That was consistent with *Sega*, which explained that

although the disassembly there involved “wholesale copying” of object code, the second factor favored fair use because the programs contained unprotected functional aspects that could not be examined without copying. 977 F.2d at 1525-26. And as the district court explained, it also follows from *Google*, which explained that “[w]here [the] copyrightable material is bound up with [the] uncopyrightable material, copyright protection is ‘thin.’” *Google*, 593 U.S. at 21. Splunk tries to distinguish *Google* on the ground that Splunk Enterprise, unlike the Java API in *Google*, is “itself a complex, creative software system.” Br. 43. But *Google* did not limit its analysis to software having its entire codebase at the periphery of copyright. *Google*, 593 U.S. at 27-29.

Factor 3. The district court correctly concluded that the third fair-use factor—the amount and substantiality of the portion of the copyrighted work used—was entitled to little weight because copying the entirety of Splunk Enterprise was “reasonable in relation to the use,” given that “the functional elements of Splunk Enterprise [that] were bound up with the creative elements.” Appx60-61; *see Campbell*, 510 U.S. at 586. Although Splunk argues the district court should have weighed the third factor more heavily against fair use, Br. 23, it does not dispute that copying the entire executable code was the only way to gain access to the functional S2S protocol—and therefore the only way to make the products interoperable. *See Sega*, 977 F.2d at 1525-27. As the district court found, “no evidence compelled the

conclusion that Splunk Enterprise was copied avoidably or for a dual purpose.” Appx61.

Factor 4. The fourth fair-use factor considers “the effect of the use upon the potential market for or value of the copyrighted work.” 17 U.S.C. § 107(4). The district court correctly deemed this factor neutral in light of the jury’s finding that “it was ‘unknown’ whether Splunk would have earned more money had Cribl not copied and used Splunk Enterprise.” Appx8 (quoting Appx41). The district court further concluded that “no evidence showed that Cribl Stream was usurping from Splunk Enterprise a copyright entitlement reserved to the copyright owner.” Appx62.

Splunk offers four arguments to the contrary. None establishes that this factor favors Splunk:

First, Splunk argues that because Cribl bears the burden of establishing fair use, the jury’s “unknown” answer disfavors fair use. Br. 38-39. That argument misconceives precedent. Cribl was required to “bring forward favorable evidence about relevant markets.” *McGucken v. Pub Ocean Ltd.*, 42 F.4th 1149, 1163 (9th Cir. 2022). Cribl did so: As the district court explained, “there was ample evidence in the trial record that Splunk customers responded to th[e] savings [created by Cribl Stream] by routing more (useful) data into Splunk Enterprise, which could increase their licensing fees paid to Splunk.” Appx8. The jury’s “unknown” answer therefore

did not reflect a failure of proof by Cribl; it reflected Splunk’s failure to persuade the jury that Cribl’s use caused Splunk harm. Nor did Splunk show that “if the challenged use should become widespread, it would adversely affect the potential market for the copyrighted work.” *McGucken*, 42 F.4th at 1163. The district court thus committed no error in finding that this factor favored fair use. *Compare Dr. Seuss Enters., L.P. v. Penguin Books USA, Inc.*, 109 F.3d 1394, 1403 (9th Cir. 1997) (deeming factor to disfavor fair use given defendants’ “failure to submit evidence on this point”).

Second, Splunk argues that any evidence Cribl increased demand for Splunk Enterprise is legally irrelevant because a “boon” to the original work does not make copying fair. Br. 39-40. Again, Splunk misunderstands the precedents it cites. The Supreme Court’s point in the cited footnote of *Campbell* was that the mere fact that copying increased demand for the original work will not necessarily establish fair use depending on the other factors—such as in the case of a “film producer’s appropriation of a composer’s previously unknown song that turns the song into a commercial success.” 510 U.S. at 590 n.21. But no binding authority supports the view that in assessing the impact of copying on the potential market for a copyrighted work, a court may only consider negative effects while blinding itself to all positive effects.

Moreover, Splunk simply brushes aside the district court's separate conclusion that the evidence showed that Cribl Stream's competitive success was attributable to replicating unprotected functional elements of Splunk Enterprise, not copying protected elements. Appx63. No cited authority casts doubt on the relevance of that consideration. Much to the contrary, losing market share due to replication of nonprotectable elements is not a cognizable harm under the Copyright Act. *See Google*, 593 U.S. at 35; *Campbell*, 510 U.S. at 592; *see also Sega*, 977 F.2d at 1523-24.

Third, Splunk argues the district court erred in failing to apply a presumption of market harm under *De Fontbrune v. Wofsy*, 39 F.4th 1214, 1226 (9th Cir. 2022). Br. 39. But as Splunk admits, that presumption applies only when the use is non-transformative. Here, the jury found the use transformative, Appx41, and Splunk does not claim that finding lacked substantial evidence.

Fourth, Splunk argues that Cribl used the entirety of Splunk Enterprise to support a competing product. Br. 40-41. But the amount copied falls under the third factor and is entitled to little weight for the reasons given above.²

² *Amicus curiae* Synopsys, Inc. erroneously asserts that fair use requires a "mutual understanding" about permissible use. Br. 6. That makes no sense given that fair use is relevant only where the copying is unauthorized. And Synopsys's suggestion that competition between the parties weighs against fair use, *id.* at 10-11, is inconsistent with *Sega* and *Sony*. *Sega*, 977 F.2d at 1522-23; *Sony*, 203 F.3d at 606-07.

* * *

As the district court concluded, “all told . . . the four statutory factors clearly favor Cribl,” Appx8, and thus Cribl’s copying for purposes of developing and maintaining interoperability (through reverse-engineering, testing, and troubleshooting) was fair use protected by Section 107 of the Copyright Act. The court’s decision was well grounded in the jury’s unchallenged factual findings, including that reverse-engineering was the only means of determining the S2S protocol, that no alternative protocol was viable, that the public benefited from Cribl’s copying, and that the use was transformative. Appx40-41 (Phase One Verdict Form Nos. 1-2, 4, 6-7).

II. THE DISTRICT COURT DID NOT ERR IN ITS INTERPRETATION OF THE SGT OR TAP AGREEMENT

Splunk challenges the district court’s construction of the contracts, but its arguments lack merit.

With respect to the SGT, the district court instructed the jury that under Section 9(a) of that agreement, Cribl was not permitted to “reverse engineer [Splunk Enterprise] (except to the extent specifically permitted by statutory law),” but that the parenthetical exception allowed for fair use, and the court reminded the jury that Cribl’s reverse-engineering, testing, and troubleshooting qualified as fair use. Appx24-25. The court also instructed the jury, however, to decide whether those activities, as well as marketing activities, breached other restrictions in Section 9

against using Enterprise for competitive monitoring or for purposes other than “internal business purposes.” Appx3955-3958. The jury ultimately returned an ambiguous verdict finding that Cribl committed some breach but awarding no actual damages. Appx16, Appx44-45. Balancing the equities and considering the public interest, the district court then enjoined only marketing activities, which it had not found to be fair use, because “downloading and running Splunk Enterprise to market Cribl Stream was not necessary for Cribl to access Splunk Enterprise’s functional elements and to develop its own interoperable, compatible software with its own distinct purpose.” Appx9.

With respect to the TAP Agreement, the district court instructed the jury that although the agreement did not afford Cribl the same fair-use protection for reverse-engineering, Section 3.3 granted Cribl a license to use Splunk Enterprise “to test [Cribl Stream]” and “to undertake other lab uses of [Splunk Enterprise] relating to the development and testing of [Cribl Stream].” Appx3953. It further instructed that the general prohibition on reverse-engineering in Section 4 did not apply to that authorized activity. The jury then found that the Cribl had not breached the TAP Agreement.

Splunk identifies no error in the district court’s interpretation of the agreements. Its rulings should be affirmed.

A. The District Court Did Not Err in Its Interpretation of the SGT

The district court correctly construed Section 9(a) of the SGT to allow Cribl’s reverse-engineering activities in connection with ensuring interoperability. In relevant part, Section 9(a) of the SGT provides that Cribl will not “reverse engineer (except to the extent specifically permitted by statutory law), decompile, disassemble or otherwise attempt to discover . . . underlying structures” of Splunk Enterprise. Appx4172 (SGT § 9(a)). The district court interpreted the SGT’s parenthetical phrase “except to the extent specifically permitted by statutory law” to include the “fair use exception of the Copyright Act” under 17 U.S.C. § 107 and thus concluded that Cribl’s “reverse engineering” was permitted by Section 9(a). Appx24-25.

That interpretation was correct. To state the obvious, the fair-use doctrine is contained in a statute that specifically authorizes the use of copyrighted material where the requirements for fair use are met, including through reverse-engineering. It therefore satisfies the plain language of Section 9 of the SGT. Although Splunk objects that the statute does not specifically reference reverse-engineering, Br. 44, the district court correctly observed that there is no other statute that the parties could “reasonably have [had] in mind.” Appx73. On appeal, Splunk points to no statute that more specifically authorizes reverse-engineering of software code.

Without identifying any reasonable alternative construction, Splunk raises on

appeal the same meritless arguments that it raised below.

First, Splunk argues the district court’s interpretation of the SGT was erroneous because fair use is merely a defense to a claim of copyright infringement, “not affirmative permission to engage in particular conduct,” Br. 44-45, by which Splunk seems to mean permission that would override a contractual prohibition. Splunk has pointed to no statute that operates in that manner, so it is not reasonable to construe the exception that way. Further, as the district court explained, if the parties intended to “contract[] away [the] statutory protection” in Section 107, Section 9 was an exceptionally “strange” way to do it. Appx73.

Second, Splunk argues the district court read similar language in the TAP Agreement inconsistently. Br. 45-46. But the district court found the agreements’ language materially dissimilar. In that view, the TAP Agreement provision bars reverse-engineering “except to the extent expressly permitted by applicable law *notwithstanding a contractual prohibition to the contrary.*” Appx1141 (emphasis added). The italicized language signals that the clause refers only to any “applicable law” (not just a statute) that overrides a contractual prohibition, such as common-law or equitable doctrines barring anti-competitive provisions as against public policy. Thus, the district court concluded “the TAP License included an extra clause recognizing that the contract could relinquish fair use rights otherwise available.” Appx69. Splunk does not acknowledge, much less explain any error in, that

distinction.

Accordingly, the relevant canon here is not to construe similar language consistently, Br. 45, but to give effect to materially different or additional language in otherwise similar provisions. *Ford v. The Silver F, Inc.*, 110 Cal. App. 5th 553, 569 (2025). At any rate, Splunk does not explain why, even if the two provisions should be construed identically, that would favor Splunk’s reading. Any ambiguity would be resolved against Splunk as the drafter. Cal. Civ. Code § 1654; *Sutter Home Winery, Inc. v. Vintage Selections, Ltd.*, 971 F.2d 401, 406 (9th Cir. 1992); *accord Gardiner, Kamya & Assocs. v. Jackson*, 467 F.3d 1348, 1352 (Fed. Cir. 2006).

Third, Splunk argues that, even if the SGT’s parenthetical in Section 9(a) permits fair use, it applies only to “reverse engineer[ing],” and not to decompiling, disassembling, or the rest of the clause. Br. 46. But reverse-engineering often requires the techniques of decompiling or disassembling. *Sega*, 977 F.2d at 1514-15 (treating decompiling and disassembling as forms of reverse-engineering); *see also Atari Games Corp. v. Nintendo of Am., Inc.*, 975 F.2d 832, 843-44 & n.6 (Fed. Cir. 1992) (describing “reverse engineering” process as involving “disassembly” and “the reverse of compilation”). Splunk’s own witness admitted as much. Appx2266-2267. The district court therefore reasonably concluded that the SGT’s permission to reverse-engineer encompasses the ordinary techniques used to do so, Appx74, including some decompiling and disassembly. For that reason, the placement of

“decompiling” and “disassembly” after the parenthetical did not bar decompiling or disassembly undertaken for reverse-engineering purposes. At minimum, any ambiguity under this provision would be construed against Splunk. *Sutter Home Winery*, 971 F.2d at 406.

Fourth, Splunk objects to the district court’s post-trial conclusion that other Section 9 use prohibitions—on “us[ing] an Offering for . . . any purpose other than [a user’s] own Internal Business Purposes” and on “access[ing] or us[ing] any Offering in order to monitor its availability, performance, or functionality for competitive purposes”—do not override Section 9(a)’s permission of Section 107’s statutory fair uses of Splunk Enterprise. Br. 46-47; Appx12, 15-16. As an initial matter, the interpretation was of no consequence to the outcome because the district court considered injunctive relief assuming the broadest possible liability (*i.e.*, all accused activities breached the SGT) and still found only a narrow injunction warranted. Appx16. But in any event, the district court’s reasoning was sound. Splunk’s interpretation would negate the SGT’s express preservation of statutory fair-use rights. As the district court put it: “Why go through the trouble of spelling out how the SGT contract preserved the extent to which statutory law protects reverse engineering if such restrictions could override and disallow this anyways?” Appx16. At the very least, again, any ambiguities must be construed against Splunk as the drafter.

For the foregoing reasons, this Court should reject Splunk’s arguments and affirm the district court’s interpretation of the SGT. But should the Court reverse the district court’s construction, the record presents an alternative ground to affirm the scope of the injunction and the denial of a new trial (the only appealable decisions even allegedly affected by Splunk’s SGT-related arguments): As Cribl argued below, the SGT is not sufficiently clear to waive Cribl’s statutory fair-use rights. Appx1047-1050. Courts applying California law, which governs the SGT, have held that “waiver of federal statutory rights must be clear and unambiguous.” *Choate v. Celite Corp.*, 215 Cal. App. 4th 1460, 1466 (2013) (collective bargaining agreement); accord *Metro. Edison Co. v. N.L.R.B.*, 460 U.S. 693, 708 (1983) (“[W]e will not infer from a general contractual provision that the parties intended to waive a statutorily protected right unless the undertaking is ‘explicitly stated.’”). Even if it were theoretically possible to waive fair use in a contract, the vague language here—in a clickwrap (at best) adhesion contract—would not be sufficient. At minimum, the Court should remand for the district court to address that argument in the first instance.

B. Splunk Forfeited Its Meritless Argument Under The TAP Agreement

The district court also correctly interpreted the TAP Agreement to permit Cribl to engage in the activities authorized under Section 3.3 (related to developing and testing Cribl Stream), including reverse-engineering, notwithstanding the

general bar on reverse-engineering in Section 4.

Section 3.3 of the TAP Agreement granted Cribl a license to download copies of Splunk Enterprise and use it to test Splunk software “for purposes of developing TAP Extensions and to test TAP Extensions[’] use with Splunk Software . . . and to undertake other lab uses of the Splunk Software relating to the development and testing of TAP extensions[.]” Appx5109-5110. It is undisputed that Cribl Stream is a “TAP extension.” Appx5108. Section 4 in turn provides that, “[u]nless otherwise expressly permitted by Splunk,” the TAP partner would not “decompile, disassemble or reverse-engineer the Splunk Software.” Appx5109-5110. (emphasis added).

The district court properly construed those provisions together to mean that the TAP Agreement allows development and testing of Cribl Stream even it involves activities like reverse-engineering otherwise barred by Section 4. Appx22-23. Although Section 4 presumptively prohibits “decompil[ing], disassembl[ing], or reverse-engineer[ing]” Splunk Enterprise, *id.*, it does not prohibit these activities where Splunk has expressly permitted them, which Section 3.3 does with respect to developing and testing TAP extensions. Appx22-23; Appx5110. The district court’s reading gives effect to both provisions, because Section 4 still prohibits reverse-engineering for other purposes.

Splunk now argues that the prefatory paragraph in Section 3 compels the opposite reading: that anything otherwise permitted by Section 3.3 is barred if listed

in Section 4. The prefatory paragraph states that the various licenses granted to Cribl in the subsections of Section 3 are “[s]ubject to TAP’s compliance with the Agreement (including the restrictions set forth in Section 4[.]].” Appx5109. According to Splunk, that means that none of the activities expressly authorized in Section 3.3 are permissible if they are also listed in Section 4.

As a threshold matter, the district court correctly concluded that Splunk forfeited that argument by failing to raise it in a Rule 50(a) motion. Appx69; *see* Fed. R. Civ. P. 50(b). Splunk’s Rule 50(a) motion did not rely on the contention raised here—that the prefatory paragraph in Section 3 subjected Section 3.3 to the limitations in Section 4. Appx69; *see also* Appx1182 & n.2.

Splunk contends its new argument was simply a “logical extension” of its original argument that Cribl breached Section 4, citing *EEOC v. Go Daddy Software, Inc.*, 581 F.3d 951, 962 (9th Cir. 2009). Br. 51-52. But *Go Daddy* is inapposite. There, the only question was whether a Rule 50(a) argument that an employee’s complaints had not been relayed to his superiors logically encompassed the argument the complaints could not have been a motivating factor behind the adverse employment decision if the superiors had never received them. *Go Daddy*, 581 F.3d at 962. The Ninth Circuit unsurprisingly concluded that the lack of causation was the necessary implication of the preserved argument. This case is totally different: In its Rule 50(a) motion, Splunk simply did not rely on the supremacy of the

contractual provision that it now cites as entitling it to relief. That is a clear forfeiture. Indeed, in *GoDaddy* itself the Ninth Circuit went on to hold that no other causation arguments had been preserved. *Id.* at 962-63.

At any rate, the argument is meritless. Read in context, the prefatory clause to Section 3 does not indicate that the Section 4 activities are carveouts from the licenses granted in Section 3's subsections. Rather, the language "[s]ubject to" merely indicates that the grants of the licenses are conditioned on compliance with the Section 4 restrictions (and all other provisions of the TAP Agreement). In marked contrast, the qualifying language in Section 4—"[u]nless otherwise permitted by Splunk"—unmistakably signals a carveout to the prohibitions set forth in that section. And because Section 3.3 is clearly an express permission to use Splunk software to develop and test extensions, it naturally falls within that qualifying language.

In short, by far the most natural and harmonious reading of Sections 3 and 4 together are that the grant of the Section 3 licenses are conditioned on compliance with other provisions of the TAP Agreement (including Section 4), but that Section 4 does not prohibit activities that fall within the scope of the Section 3 licenses even if they are listed in Section 4. That reading gives effect to both provisions, and it accounts for the difference in language between the two qualifying clauses (*i.e.*, "subject to" vs. "unless otherwise permitted"). Had the drafters intended Section 4

prohibitions to effectively diminish the Section 3 licenses, they could easily have written “Unless prohibited by Section 4” at the beginning of Section 3, and they almost assuredly would have changed the broad qualifying language in Section 4 to exclude the Section 3.3 licenses. At minimum, any ambiguity should be construed against Splunk as the sole drafter.

Splunk’s reading would also render other provisions of Section 3.3 nullities. For example, Section 3.3 authorizes Cribl to “make up to five (5) copies” of Splunk software for testing purposes, but Section 4 prohibits Cribl from “copy[ing] any Splunk Software (except as required to run the Splunk Software and for reasonable backup purposes).” Appx5110. Under Splunk’s theory that Section 4 restrictions trump Section 3.3 licenses, the five-copy provision would have no effect. Similarly, Section 4 flatly prohibits Cribl from “disclos[ing] . . . Splunk Software to any third party,” but Section 3.3 allows Cribl to “demonstrate the use of TAP Extensions with the Splunk Software to actual, potential or prospective Users” under certain conditions. Appx5110. Clearly, Section 3.3 is a carveout to Section 4, not vice versa.

Splunk separately argues that Section 3.3 does not “expressly” permit reverse-engineering because it does not contain those precise words. The district court correctly rejected that hyper-literal view. Appx67-68. As the district court explained, Section 3.3 grants permission to use Splunk’s software to “test the Splunk Software for purposes of developing TAP extensions,” which includes permission to engage

in conduct reasonably necessary to do so, such as reverse-engineering and troubleshooting. Appx68. The word “expressly” ensures that exceptions will not be inferred by implication, but conduct that falls within the plain language of Section 3.3—such as developing and testing extensions through reverse-engineering—easily qualifies.

Splunk also invokes the specific-governs-the-general canon, arguing that the TAP Agreement’s “specific and explicit” prohibition on reverse-engineering “cannot be overridden by” Section 3.3’s “general permission” to test extensions. Br. 51. But neither provision is more specific than the other—they are a Venn Diagram of partially overlapping activities (reverse-engineering and developing TAP extensions)—so that canon has no application here. And at any rate, the canon applies only “when provisions are inconsistent,” *Southern Cal. Gas Co. v. City of Santa Ana*, 336 F.3d 885, 891 (9th Cir. 2003), but the provisions are readily harmonized in light of their distinct prefatory language.

* * *

The Court should reject Splunk’s challenges to the district court’s construction of the SGT and the TAP Agreement.

III. EVEN IF THE DISTRICT COURT ERRED WITH RESPECT TO THE COPYRIGHT OR CONTRACT CLAIMS, THERE ARE NO GROUNDS FOR A NEW TRIAL ON DAMAGES OR A REVISED INJUNCTION

Even if the Court concludes that the district court erred on the copyright or contract claims, a new damages trial would not be warranted. Splunk has not challenged on appeal the jury’s finding that it was “unknown” whether Splunk would have earned more money had Cribl not copied Splunk Enterprise. Appx41. That finding—returned before any instruction on what activities constitute fair use under copyright law or substantive contract issues—alone forecloses any award of damages to Splunk. That disposes of Splunk’s request for a new damages trial.

With respect to the injunction, even if this Court were to reverse the district court’s construction of the TAP Agreement, no injunction would be warranted. As Splunk acknowledges, the TAP Agreement was terminated in November 2021. Br. 10. As a result, “injunctive relief based upon that contract is moot.” *TNS Media Res., LLC v. Tivo Res. & Analytics, Inc.*, 629 F. App’x 916, 937 (Fed. Cir. Sept. 16, 2015); *see also Carbon Fuel Co. v. United Mine Workers of Am.*, 444 U.S. 212, 214 n.2 (1979).

As for the SGT, the jury found that Cribl had breached the agreement, and the instructions permitted the jury to find that Cribl’s fair-use activities were breaches. Appx3955. At Splunk’s urging, the district court “[a]ssum[ed], *arguendo*” the “broadest possible finding of liability” (*i.e.*, all activities breached the SGT) in

fashioning injunctive relief, but enjoined only marketing uses because “the balance of the hardships as well as the public interest militate[d] against the broadest possible injunction,” not because it interpreted the jury’s verdict narrowly. Appx16. Thus, the district court’s interpretation of Section 9(a) that Splunk challenges on appeal was immaterial to the result.

IV. THE DISTRICT COURT CORRECTLY FOUND THE ’443 AND ’438 PATENTS PATENT-INELIGIBLE UNDER 35 U.S.C. § 101

The district court correctly dismissed Splunk’s patent-infringement claims under Section 101 of the Patent Act.

On appeal, Splunk relies only on U.S. Patent Nos. 9,762,443 (“the ’443 patent”) and 10,805,438 (“the ’438 patent”). Although the ’438 and ’443 patents are from separate patent families, both relate to computer networks—specifically to configuring a system for capturing and processing network data across a distributed network environment. Splunk does not challenge the district court’s finding that “[t]he representative claims of the ’438 and ’443 patents disclose methods implemented in a distributed arrangement involving at least one configuration server and one remote capture agent (‘RCA’).” Appx92.

Applying the correct legal standard, the district court identified the fatal problem with the representative claims: They are written at a purely functional, result-oriented level that describes *what* the claimed methods do, not *how* they do it. Indeed, although Splunk repeatedly asserts that the claims recite the “how,” it does

not identify any claim language that does so. *E.g.*, Br. 55. Because the district court also correctly found that the claims do not disclose an inventive concept, the district court’s dismissal should be affirmed.

A. *Alice* Step One: The Claims Are Directed to Abstract Ideas

In cases involving networked computers, this Court has drawn a bright line. On one side “are claims that simply call for the use of computers and networks as tools to carry out an abstract idea, using their ordinary functions without specific hardware or process advances in those functions—*e.g.*, receiving inputs, storing and retrieving, processing, outputting (including displaying), and transmitting.” *GoTV Streaming, LLC v. Netflix, Inc.*, 166 F.4th 1053, 1064 (Fed. Cir. 2026). On the other side “are claims that call for a concrete asserted improvement in *how* those functions are carried out, which requires more than result-focused functional language and more than just using those functions in the context of specifically identified content.” *Id.* Here, the district court correctly found that the representative claims of the ’438 and ’443 fall squarely on the first, patent-ineligible and abstract side of that line, and Splunk offers no basis for this Court to disturb that ruling.

1. The District Court Correctly Characterized the Claims at the Appropriate Level of Abstraction

A patent ineligibility analysis depends on “the language of the [] [c]laims themselves”; thus, “only features that are claimed, not unclaimed details that appear in the specification, can supply something beyond ineligible matter.” *GoTV*

Streaming, 166 F.4th at 1060-61 (citing *ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759, 767, 769-70 (Fed. Cir. 2019)). The '438 and '443 patents both claim a single configuration server that sends instructions (“configuration information” or “configuration data”) to an RCA to generate event streams from network data.

The '438 claims provide that the configuration server generates the configuration information it sends to the RCA based on user input it receives. The district court correctly found these claims are thus “directed to the abstract idea of generating (event) data by applying (configuration) data [the RCA] receives to (network) data it monitors.” Appx94.

Similarly, the '443 claims provide that the RCA uses “the same configuration information” received from the configuration server for “generating” and “transforming” timestamped event data, and the district court correctly found these claims are thus “directed to the abstract idea of monitoring (network) data and applying (configuration) data received to generate and transform (event) data.” Appx94.

Splunk argues the district court erred in finding the claims abstract because they “provide specific, technological solutions” for “how a computer network is organized [to] improv[e] data capture to be compatible with modern, cloud-based systems.” Br. 55. But, as the district court noted, “the claims themselves do not disclose performing any ‘special data conversion’ or otherwise describe how the

alleged goal—‘fixing the conventional, inflexible approach to capturing and analyzing network data’—is achieved.” Appx94 (citing *Hawk Tech. Sys., LLC v. Castle Retail, LLC*, 60 F.4th 1349, 1357 (Fed. Cir. 2023)) (internal quotation marks and citations omitted). The district court further observed that “neither the claim language nor the specification language provides guidance on *how*” the RCA monitors and performs operations on event data. *Id.* (emphasis in original).

That analysis was correct and controlling. This Court has routinely “held claims using purely ‘result-focused functional language, containing no specificity about how the purported invention achieves those results,’ to be directed to an abstract idea.” *GoTV Streaming*, 166 F.4th at 1064 (citing *Beteiro, LLC v. DraftKings Inc.*, 104 F.4th 1350, 1356 (Fed. Cir. 2024)); *see also Two-Way Media Ltd. v. Comcast Cable Commc’ns, LLC*, 874 F.3d 1329, 1337 (Fed. Cir. 2017) (holding claims requiring “functional results of ‘converting,’ ‘routing,’ ‘controlling,’ ‘monitoring,’ and ‘accumulating records’” without “sufficiently describ[ing] how to achieve these results in a non-abstract way” were abstract and patent-ineligible).

Splunk argues that the district court “oversimplif[ied]” the claims. But Splunk does not identify any “stripp[ed] away” limitation that explains how any of the claimed functional results are accomplished. Br. 56. Although Splunk asserts that the district court ignored the claims’ supposed recital that “agents parse data using protocol-specific rules delivered by a configuration server,” *id.*, this formulation of

the claim language—like the operative claimed steps the district court analyzed—describes only *what* the agent receives and *what* output it produces, not *how* protocol-specific rules are generated, applied to live network traffic, or used to segment and transform packet data. That is precisely the result-oriented functional language this Court has repeatedly found insufficient for patent eligibility.

2. The District Court Correctly Found the Claims Do Not Improve Computer Functionality

The '438 and '443 patents' claims are also abstract because they recite an RCA that processes network traffic no differently than conventional network capture products. As the district court correctly observed, Splunk's own patents acknowledge "conventional" network capture devices already processed network packets into events. *See* Appx95; Appx173 (1:41-67, 2:1-19); Appx136 (1:13-41) (noting conventional capture devices perform "Extraction, Transform, and Load" processes on network traffic data to filter, transform and/or aggregate network data).

Splunk asserts, without citing the claims or specifications, that the purported inventions improve the "scalability, adaptability, and bandwidth efficiency" of network-capture technologies by "orchestrating distributed capture and transformation in a protocol-aware, configurable manner." Br. 55-56. That arguments fails for at least four reasons.

First, only the '438 representative claim recites a "protocol" at all. Appx184 (24:32-37).

Second, both representative claims are satisfied by a *single* RCA. Br. 2. They therefore are not directed to a scalable solution involving many distributed RCAs.

Third, the specifications do not state that conventional network-capture technologies were *unable* to capture and transform data in an adaptable and configurable manner. Rather, they merely say that “most” (but not all) conventional technologies “operate in a fixed way” and that the purported invention “includes functionality to perform protocol-based capture and analysis of network data,” without describing *how* to implement that functionality. *See* Appx138 (6:60-64); Appx175 (6:20-24); Appx176 (7:22-38).

Finally, the only *claimed* reduction of network traffic is that which results from transmitting event data culled from, and in lieu of, network packets, and the specification makes clear that this activity was not itself unconventional. *See* Appx173 (1:37-41). In any event, as this Court has held, Splunk’s contention that the claims improve bandwidth efficiency, even if true, is irrelevant because the claims do not describe how this alleged improvement is achieved. *See Hawk Tech.*, 60 F.4th at 1357 (holding claims that do not disclose how to achieve the supposed goal of “conserving bandwidth while preserving data” are abstract).

Splunk’s remaining argument at *Alice* step one is that the centralized delivery of instructions (*i.e.*, configuration information or data) over a network itself constitutes a computer improvement. *See* Br. 54-55 (stating “[b]oth patents recite a

concrete architecture: a central server generates configuration data; distributed agents receive it and apply it in real-time at the edge” and arguing “these claims are not directed to merely ‘monitoring and transforming data’” but “to remote protocol-aware monitoring and transformation, techniques tailored for high-volume, distributed systems”). It does not. As in *GoTV Streaming*, “the claims do not call for any new hardware, whether at the server end, the [RCA] end, or the networks that connect them.” 166 F.4th at 1065-66. Nor do the claims “call for any improvement in ordinary computer (here, server) functions, such as receiving, storing, processing, outputting, and transmitting.” *Id.* “Given what is taught in the Asserted Patents themselves—and, most particularly in this case, what is *not* taught, which in context reinforces that a person of ordinary skill in the art would have recognized the claims to involve nothing more than conventional, routine, and well-understood use of [RCAs]—no amount of creative pleading could have succeeding in transforming the claims into patent-eligible subject matter[.]” *Beteiro*, 104 F.4th at 1358.

The claims here are like those found ineligible in *ChargePoint*, which involved claims directed to improved networked charging stations for electric vehicles by management with a centrally located server. 920 F.3d at 767. In *ChargePoint*, “the problem perceived by the patentee was a lack of a communication network for these charging stations.” *Id.* at 768. Here, Splunk similarly argues the problem it overcame was a lack of communication network for its RCAs. *See* Br. 4,

54-56. This Court found the claims in *ChargePoint* were abstract because the specification did not suggest that the charging station “is improved from a technical perspective” or “would operate differently than it otherwise could,” or “that the invention involved overcoming some sort of technical difficulty in adding networking capability to the charging stations.” 920 F.3d at 768. The same is true here of the claimed RCAs. *See* Appx136 (1:30-41); Appx138 (6:60-64); Appx173 (1:65-2:9); Appx175 (6:20-24); Appx176 (7:22-38).

Although *ChargePoint* is squarely on point, Splunk primarily relies on two cases that are both readily distinguishable. In *Packet Intelligence LLC v. NetScout Systems, Inc.*, 965 F.3d 1299, 1309-10 (Fed. Cir. 2020), the asserted claims were directed to identifying disjointed “connection flows” as belonging to a single “conversational flow”—a classification prior-art network monitors could not perform—which the Court held was a specific improvement in computer technology rather than an abstract idea. That is qualitatively different from configuration delivery over a conventional, distributed network. *Cf. id.* at 1309 (claim “purports to meet a challenge unique to computer networks”).

Likewise, in *SRI International, Inc. v. Cisco Systems, Inc.*, 930 F.3d 1295, 1304 (Fed. Cir. 2019), the asserted patent claims “over[rode] a routine and conventional sequence of events”; here, the claims only describe what any conventional network capture device does, merely adding a connection to an

upstream configuration server over a conventional network. *Cf. id.* (noting *SRI* “claims actually prevent the normal, expected operation of a conventional computer network”); *see also Cisco Sys., Inc. v. Uniloc 2017 LLC*, 813 F. App’x 495, 498 (Fed. Cir. May 13, 2020) (noting claims in *SRI* were not abstract because they recited “a specific technique for improving computer network security”).

Because the ’438 and ’443 patents’ claims fall squarely on the “tools to carry out an abstract idea” side of the bright line for patent eligibility this Court described in *GoTV Streaming*, 166 F.4th at 1064-65, the district court’s judgment against Splunk on Counts I and II of its complaint should be affirmed unless Splunk can demonstrate an inventive concept that would salvage these patent claims. As explained below, they cannot.

B. *Alice* Step Two: The Claims Recite No Inventive Concept

“In conducting the [*Alice*] step-two inquiry, [this Court has] repeatedly emphasized that it is not sufficient, in order to pass muster, for a claim to use functional, result-focused language or to encompass ordinary computers and networks to perform their ordinary functions in carrying out an abstract idea, even when narrowed to a particular use or environment (such as particular subject matter), without going further to require a specific implementation to improve *how* those functions are carried out.” *GoTV Streaming*, 166 F.4th at 1067; *see also US Patent No. 7,679,637 LLC v. Google LLC*, 164 F.4th 1373, 1379-80 (Fed. Cir. 2026)

(“Merely describing the functions of the abstract idea itself, without particularity, . . . is simply not enough under step two.” (citation omitted)).

Splunk’s arguments that the representative claims express an inventive concept, Br. 57, are merely conclusory, lacking any suggestion of *how* or *why* the claim language describes anything more than abstract ideas. *See Trinity Info Media, LLC v. Covalent, Inc.*, 72 F.4th 1355, 1365-66 (Fed. Cir. 2023) (disregarding conclusory allegations regarding patent claim’s inventive concept when evaluating dismissal under Rule 12(b)(6)). The ordered combination Splunk claims is inventive here—(1) a generic server generates configuration data, (2) the server sends the configuration data to an RCA, and (3) the RCA generates and transforms events—is a generic client-server architecture applied to network data capture that does not supply an inventive concept because each step simply describes a generic computer performing its ordinary function. The district court correctly found that the representative claims do not capture any “alleged improvement[]” and “merely apply result-oriented, abstract ideas without specifying any non-conventional way to accomplish or practice them.” Appx95-96.

Splunk nevertheless contends there is an inventive concept because the purported inventions enable “dynamic control and edge-side efficiency that prior fixed tools lacked.” Br. 57. But the district court properly found the claims do not require dynamic configuration, noting the ’443 patent “itself betrays that this is not

the claimed invention.” Appx113 (noting specification language provides that “‘most’ [(not all)] conventional network capture technologies operate in a fixed manner, and ‘generally’ [(not always)] cannot be dynamically or easily modified”) (citing Appx138 (6:60-64)). Indeed, the claim scope is broad enough to allow the configuration information to be delivered at *any* time. Appx148 (representative claim 1 has no time limitation); Appx184 (same). Splunk’s assertion that the inventions enhance “edge-side efficiency,” Br. 57, also cannot save these abstract claims. As this Court has found, “claiming the improved speed or efficiency inherent with applying the abstract idea on a computer [does not] provide a sufficient inventive concept.” *Sanderling Mgmt. Ltd. v. Snap Inc.*, 65 F.4th 698, 705 (Fed. Cir. 2023) (citation omitted).

Splunk invokes *Bascom Global Internet Services, Inc. v. AT&T Mobility LLC*, where the claims were directed to the abstract idea of filtering Internet content but were deemed eligible under *Alice* step two because they required a specific, non-conventional arrangement—filtering at a remote, central server rather than locally—that was recited in the claims with structural specificity. 827 F.3d 1341, 1350 (Fed. Cir. 2016) (“The inventive concept . . . is the installation of a filtering tool at a specific location, remote from the end-users, with customizable filtering features specific to each end user.”). Unlike in *Bascom*, the combination of steps here reflects no specific structural choice. It is simply the ordinary sequence of any client-server

interaction: a server receives input, generates instructions, and transmits them, and a remote device executes them. Indeed, the asserted claims here generally recite a conventional arrangement where data operations (*e.g.*, filtering) are performed locally by an RCA, not on a server at a single location. *See, e.g.*, Appx173 (2:5-9) (conventional network capture devices process data, including filtering, at point of capture); Appx175 (6:31-37) (claimed inventions process data, including filtering, at point of capture). Thus, *Bascom* is distinguishable for the same reasons as *ChargePoint*: “the claims do nothing to improve how [RCAs] function; instead, the claims merely add generic networking capabilities to those [RCAs] and say ‘apply it.’” *ChargePoint*, 920 F.3d at 774-75 (citation omitted).

Splunk further argues that *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350 (Fed. Cir. 2016), cited by the district court, is inapposite because, according to Splunk, Splunk’s asserted claims “require specific capture, segmentation, and protocol-aware transformation mechanics,” and “do not merely recite high-level data analysis.” Br. 58. But Splunk’s characterization of the claims is not supported by the claim language, is not supported by the claim language, which simply requires generating and transforming event data from captured network packets “based on” or “according to” configuration information, not the use of specific capture or segmentation techniques. Appx148 (26:38) (“generating, based on the configuration information”); Appx184 (24:43-45) (“generate ...

according to the configuration data”). For example, the ’443 patent’s representative claim (the only one that mentions “segmenting”) merely recites that the “generating” step includes “segmenting the at least one network packet into a plurality of events”—a functional result—without any discussion of *how* it does so, let alone does so unconventionally. Appx148 (26:40-44). Moreover, as discussed above, Splunk’s patents confirm that conventional capture technologies could filter, transform, aggregate, and/or extract data from captured network traffic, and do not assert that Splunk invented protocol-based transformation. See Appx136 (1:30-41); Appx173 (1:65-2:9). Thus, *Electric Power*’s holding that there was no inventive concept under *Alice* step two because the “claims at issue do not require any nonconventional computer, network, or display components,” 830 F.3d at 1355, applies with equal force here. Splunk’s claims fail to recite a specific implementation to improve how their ordinary functions are carried out on conventional computers and networks; thus, under this Court’s precedents, the district court’s finding that there is no inventive concept should be affirmed.

C. The District Court Did Not Err in Invalidating the Patents on the Pleadings

Finally, Splunk contends the district court erred by finding the patents ineligible at the pleading stage because there is a plausible factual dispute as to the claims’ inventive concept. But *Berkheimer v. HP Inc.*, cited by Splunk, recognizes such factual disputes only when the claim language itself plausibly recites something

that could be non-conventional. 881 F.3d 1360, 1368 (Fed. Cir. 2018) (“As our cases demonstrate, not every § 101 determination contains genuine disputes over the underlying facts material to the § 101 inquiry.”). Where the claims recite only functional results without any specific implementation (as here), there is no *Berkheimer* fact question: The “improvement” is simply not in the claims, and no amount of extrinsic evidence will change that fact. *See id.* (“Patent eligibility has in many cases been resolved on motions to dismiss or summary judgment. Nothing in this decision should be viewed as casting doubt on the propriety of those cases.”).

The district court correctly applied *Berkheimer*. It did not resolve a disputed fact about whether the RCA architecture was conventional or about the prior art; rather, it made a legal determination about claim scope, *i.e.*, that the claims do not recite the RCA architecture with sufficient specificity to make conventionality a material fact. *See Appx95-96* (“[T]he eligibility of the representative claims does not turn on the factual issue of whether the alleged improvements are well-understood, routine, and conventional ***because no alleged improvement is captured in the claim language.***” (emphasis added)).

Splunk also rehashes its prior arguments regarding patent eligibility, arguing the district court overlooked that the patents’ “protocol-specific remote capture agents, transformation logic, and centralized configuration . . . collectively improve the flexibility, scalability, and real-time responsiveness of machine data collection.”

Br. 59. Critically, although Splunk acknowledges that any such improvement must be found in the claims, it does not cite any claim language to support this argument, instead citing only the specification (*i.e.*, Appx137, Appx173, Appx341-343) and its opposition to Cribl’s motion to dismiss (Appx451-452). Br. 59-60. Moreover, as explained above, the ’438 and ’443 patents do not claim to have invented protocol-specific transformation of network data, nor do the claims require a “scalable” or “real-time” approach to processing that data. *See Aatrix Software, Inc. v. Green Shades Software, Inc.*, 890 F.3d 1354, 1357 (Fed. Cir. 2018) (emphasizing that any factual issue under 35 U.S.C. § 101 must “pertain to the invention *as claimed*” (emphasis added)).

In addition, there is no factual dispute relating to whether centralized configuration by a server over a network is an inventive concept. It is not. This Court rejected similar allegations in *ChargePoint*. There, the patentee (like Splunk here) argued it “presented sufficient factual allegations to preclude dismissal at the Rule 12(b)(6) stage” because “its patents represent an unconventional solution to technological problems in the field, and thus contain an inventive concept.” *ChargePoint*, 920 F.3d at 773. Those problems included the need for a network that facilitates real-time communication to control a remote charging station. *Id.* at 774. The Court found that “the alleged ‘inventive concept’ that solves problems identified in the field is that the charging stations are network-controlled.” *Id.* But because

“network control is the abstract idea itself . . . a claimed invention’s use of the ineligible concept to which it is directed cannot supply the inventive concept that renders the invention ‘significantly’ more than that ineligible concept.” *Id.* (citation omitted).

Similarly here, the representative claims’ recitation of conventional network communications between a server and an RCA is the only possible inventive concept; thus, because Splunk cannot establish that its patents do anything more than claim this abstract idea, there is no plausible factual dispute left to be resolved. The Court should therefore affirm the district court’s dismissal of the patent-infringement claims.

V. IN THE EVENT THE COURT DISTURBS THE JUDGMENT ON ANY COPYRIGHT ISSUE, CRIBL WAS ENTITLED TO JUDGMENT AS A MATTER OF LAW ON WILLFUL COPYRIGHT INFRINGEMENT

Should the Court disturb the judgment in any respect on the copyright or contract claims (including with respect to remedy), it should correct certain errors that the district court made in denying Cribl’s motion for judgment as a matter of law, because correcting those errors could affect the scope of proceedings on remand.

The district court should have granted Cribl judgment as a matter of law on the jury’s finding of willful copyright infringement. The trial record lacks substantial evidence that Cribl engaged in copyright infringement or acted willfully.

1. a. Copyright infringement occurs only where the alleged infringer creates “copies,” defined as “material objects, . . . in which a work is fixed . . . and from which the work can be perceived, reproduced, or otherwise communicated.” 17 U.S.C. § 101; *see id.* § 102(a); *see also CDK Glob. LLC v. Brnovich*, 16 F.4th 1266, 1276 (9th Cir. 2021). Here, Splunk failed to introduce any substantial evidence that Cribl—by running Splunk Enterprise—made a sufficiently “fixed” unauthorized copy of Splunk’s copyrighted object code to satisfy the Copyright Act.

Cribl’s downloads of Splunk Enterprise—the initial copying—were licensed under the SGT and (prior to its termination) the TAP Agreement. *See, e.g.*, Appx4169-4187 (SGT as general license subject to use restrictions); Appx5110 (TAP Agreement licensing “download[s]” of Splunk software). For that reason, an unauthorized “copy” could have been created only when Cribl executed Splunk Enterprise, which purportedly results in the copying of at least portions of the copyrighted object code into RAM. But Splunk submitted no evidence that the RAM copying created “fixed” copies of the software under the Ninth Circuit’s construction of the Copyright Act.

Under Ninth Circuit precedent, “[a] work is ‘fixed’ in a tangible medium of expression” if it meets “two distinct but related requirements: . . . the embodiment requirement and the duration requirement.” *CDK Glob.*, 16 F.4th at 1276 (quoting *Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, 536 F.3d 121, 127 (2d Cir. 2008))

(internal quotation marks omitted). Software loaded into RAM satisfies the embodiment requirement. *See MAI Sys. Corp. v. Peak Comp., Inc.*, 991 F.2d 511, 518-19 (9th Cir. 1993). But it does not necessarily satisfy the duration requirement, which distinguishes between true “copies” and mere transitory uses. *See CDK Glob.*, 16 F.4th at 1276. Applying that distinction, courts have found that plaintiffs fail to establish copying where they lack evidence that the embodiment in RAM or other storage “persist[s] for a period of more than transitory duration.” *Id.* at 1276-77 (affirming denial of preliminary injunction where plaintiffs offered “no evidence” embodiments would satisfy duration requirement); *Cartoon Network*, 536 F.3d at 129-30 (buffering data overwritten in 1.2 seconds was transitory and therefore not fixed); *see also Capitol Recs., LLC v. Escape Media Grp., Inc.*, No. 12-CV-06646 AJN SN, 2014 WL 12698683, at *21 (S.D.N.Y. May 28, 2014), *report and recommendation adopted*, 2015 WL 1402049 (S.D.N.Y. Mar. 25, 2015).

Here, Splunk proffered *no* evidence at trial—none—establishing how long Splunk Enterprise’s executable code is fixed in RAM when Cribl executes it for any of the allegedly unauthorized purposes. Splunk’s technical expert testified only to the embodiment requirement, not the duration requirement. Appx3098-3100. Further, he admitted that for “very large programs” such as Enterprise, the system would only load part of the program at any one time. *Id.* And although he opined in the abstract that this partial code is not replaced until space is needed, his testimony

confirmed that code is regularly cycled in and out of RAM. *Id.* Splunk ultimately failed to adduce any evidence showing that any protectable portion of Splunk Enterprise remained in RAM long enough, during any infringing use, to satisfy the duration requirement as construed by the Ninth Circuit.

The district court reached the opposite conclusion on the ground that the jury “could have inferred” enough persistence from expert testimony that RAM copies endured until displaced and from evidence that screen displays persisted long enough to be perceived. Appx139. That reasoning does not cure Splunk’s failure of proof. The relevant question was whether Splunk introduced substantial evidence of an infringing RAM copy, not whether a jury might speculate from generalized runtime testimony that some execution at some point persisted long enough to qualify. For example, in *CDK Global*, the Ninth Circuit found it insufficient that the embodiment allowed the copyrighted software “to process the request of the dealer or authorized integrator using it”; the fact remained that the plaintiff had still failed to show that the embodiments “persist for a period of more than transitory duration.” 16 F.4th at 1276. And the district court’s order itself acknowledged the critical point that “the copying involving the most persistence might have been done most commonly for uses that were fair uses or licensed uses,” while sustaining the verdict only on the possibility that a jury “could have inferred” similar persistence for infringing uses. Appx139. The infringement judgment cannot be sustained on the

bare possibility that at least one unauthorized RAM copy may have persisted long enough to qualify (without any evidentiary proof that it did so).

b. Splunk may ask the Court to affirm the district court’s ruling on copyright infringement on the alternative ground that Cribl made fixed infringing copies by downloading Splunk Enterprise in the first instance—even though the agreements permitted Cribl to download the software, Appx4169, Appx5110—on the theory that Cribl had the subjective intent at the time of the download to violate contractual use restrictions in the future. That theory fails as a matter of law. The SGT (which the district court held applied to all of Cribl’s downloads, including those during its participation in the TAP program, Appx51) prohibits only certain *uses* of Splunk Enterprise, not single, initial downloads with the contemplation of some future use. *E.g.*, Appx4169 (SGT § 1(A)) (“General Rights” provision regarding right “to use” offerings for internal business purposes); Appx4172 (SGT § 9) (use restrictions). And the initial downloads are necessarily completed before there has been any use of the software. They were therefore authorized.

Splunk has previously argued the SGT’s preamble makes the authorization of a download contingent on Cribl’s pre-use subjective intent, because the preamble states that by downloading the software, the user is agreeing to the SGT. Appx4169. That argument does not make sense. Even if a user contemplates a future breach when assenting to an agreement, that does not mean the user breaches the agreement

by the mere act of assent (here, downloading the software). Were it otherwise, routine preambles would render the mere consideration of committing future breaches immediately actionable. And at any rate, the fact that a dispute about the scope of authorization later arises does not mean that the user intended to breach the agreement at the time of assent. Here, for example, Cribl has vigorously contested in good faith that it ever committed a breach. Accordingly, Splunk’s “subjective intent” theory provides no alternative basis to affirm the district court’s denial of Cribl’s motion for judgment as a matter of law on copyright infringement.

2. Even if Splunk had presented sufficient evidence to establish copyright infringement, it lacked substantial evidence of willfulness. As Cribl argued below, there was no substantial evidence that Cribl actually knew its conduct infringed Splunk’s copyright, or that it acted with reckless disregard or willful blindness as to its infringement.

As an initial matter, whether Cribl’s infringement was willful had to be assessed against the narrowed field of uses that were not already held to be fair or licensed. At the time the jury found Cribl’s infringement was willful, it had been instructed that reverse-engineering, testing, and troubleshooting to support interoperability were fair uses. Appx3948. Thus, any willfulness finding had to rest on the remaining accused conduct, *i.e.*, “marketing,” which consisted of demonstrating to customers that Stream interoperated with Splunk Enterprise.

Splunk did not introduce substantial evidence that anyone at Cribl believed marketing infringed Splunk's copyrights. Rather, Cribl's internal discussions about legal risk focused on reverse-engineering and interoperability via S2S—the very conduct later held to be fair use. *See, e.g.*, Appx3358 (trial testimony of Cribl CEO acknowledging early discussions of legal risk related to developing S2S implementation); Appx5218-5219 (Slack discussion of legal risk surrounding implementing S2S protocol); Appx5199 (discussing minimizing discussion of S2S integration with potential customers). Evidence of concern about being sued over reverse-engineering the S2S protocol (a protected fair use activity) is not evidence of knowledge that marketing-related uses of Splunk Enterprise would infringe Splunk's copyrights and fall outside of the fair-use doctrine.

The district court nevertheless stated that because Cribl's founders understood copyright law well enough to discuss reverse-engineering, the jury could infer they also knew their “less innovative uses” for marketing “all but certainly crossed the line,” and avoided learning more before “walking right over it.” Appx65. But the existence of legal discussions about one category of use—interoperability-related copying—does not amount to substantial evidence of actual knowledge or recklessness as to a distinct category of use, especially by non-attorneys.

That disconnect is especially glaring because the record evidence shows Cribl operated for four years under the TAP Agreement, which expressly allowed Cribl to

demonstrate interoperability of TAP extensions with Splunk Software to actual and prospective users. Appx5110. The district court in fact acknowledged that TAP partners were “allowed to use Splunk Enterprise to market these newly developed services.” Appx51. Once the TAP Agreement was terminated, the parties disputed the extent to which remaining SGT rights and statutory fair use still permitted related conduct, but that sort of legal uncertainty cuts against willfulness. In the absence of substantial evidence that Cribl actually knew, or recklessly disregarded, that running Splunk Enterprise to demonstrate to customers the interoperability between Splunk Enterprise and Cribl Stream was not a protected fair use, the district court should have set aside the jury’s willfulness verdict.

CONCLUSION

The Court should affirm the judgment and injunction below. To the extent it disturbs either with respect to any copyright-related issues, it should reverse the district court’s denial of Cribl’s motion for judgment as matter of law on the grounds set forth above.

DATED: July 17, 2026

Respectfully submitted,

QUINN EMANUEL URQUHART &
SULLIVAN, LLP

By: */s/ John F. Bash*

John F. Bash

*Attorneys for Defendant-Cross-Appellant
Cribl, Inc.*

CERTIFICATE OF SERVICE

I hereby certify that on July 17, 2026, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Federal Circuit by 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.

Dated: July 17, 2026

By: /s/ John F. Bash

John F. Bash

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Federal Circuit Rule 32(b)(1) because it contains 15,994 words, excluding the portions of the brief exempted by Federal Rule of Appellate Procedure 32(f) and Federal Circuit Rule 32(b)(2).

2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type style requirements of Federal Rule of Appellate Procedure 32(a)(6) because it has been prepared in a proportionally-spaced typeface using Microsoft Word in 14-point Times New Roman font.

Dated: July 17, 2026

By /s/ John F. Bash

John F. Bash