Nos. 2016-1916, 2016-2007

IN THE UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

CONTENTGUARD HOLDINGS, INC.,

Plaintiff-Appellant,

v.

APPLE INC.,

Defendant-Cross-Appellant.

Appeal from the United States District Court for the Eastern District of Texas in Case No. 2:13-cv-01112, Judge Rodney Gilstrap

PRINCIPAL AND RESPONSE BRIEF OF DEFENDANT-CROSS-APPELLANT APPLE INC.

Constantine L. Trela, Jr.
David T. Pritikin
Nathaniel C. Love
SIDLEY AUSTIN LLP
One South Dearborn Street
Chicago, IL 60603
(312) 853-7000

Jeffrey P. Kushan
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
(202) 736-8000

Counsel for Apple Inc.

November 14, 2016

CERTIFICATE OF INTEREST

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

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

Apple Inc.

2. The names of the real parties in interest represented by me are:

See response to number 1.

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

Apple Inc. discloses that it has no parent corporation and that no publicly held corporation owns 10% or more of its stock.

4. The names of all law firms, and the partners or associates, that appeared for the party represented by me in the trial court or are expected to appear in this Court and who are not already listed on the docket for the current case are:

Bryan K. Anderson, David L. Anderson, Bryan A. Blumenkopf*, Scott M. Border, Thomas A. Broughan III, Richard A. Cederoth, Theodore W. Chandler, Michael R. Franzinger, Nathan Greenblatt, Kelly A. Krellner*, Ryan N. Phelan*, Carter G. Phillips, Wonjoo Suh, John P. Wisse, Sidley Austin LLP; Melissa R. Smith, Gillam & Smith LLP.

November 14, 2016 /s/ Constantine L. Trela, Jr.

Constantine L. Trela, Jr.
SIDLEY AUSTIN LLP
One South Dearborn Street
Chicago, IL 60603
(312) 853-7000

Counsel for Apple Inc.

* No longer affiliated with Sidley Austin LLP

TABLE OF CONTENTS

Page

JURISDICTIONAL STATEMENT 1

COUNTERSTATEMENT OF ISSUES 7

COUNTERSTATEMENT OF THE CASE 7

I. INTRODUCTION 7

II. STATEMENT OF FACTS 10

A. Digital Rights Management. 10

B. ContentGuard's Trusted Systems Patents. 11

1. Repositories. 12

2. The Communications Integrity Requirement. 14

3. Usage Rights. 16

4. ContentGuard's Meta-Rights Patent. 18

C. Apple's iTunes/FairPlay System. 18

III. PROCEEDINGS BELOW 22

A. The Parties' Claims. 22

B. Claim Construction. 22

C. Discovery Disputes. 24

1. ContentGuard's Source Code Production Complaints. 24

2. Discovery Concerning Updates to FairPlay Servers. .. 25

D. Trial and Jury Verdict. 26

1. The District Court Resolves the rsync Issue. 26

2. The Jury Finds Apple Does Not Infringe. 28

SUMMARY OF ARGUMENT 31

ARGUMENT 34

I. STANDARD OF REVIEW 34

II. THE DISTRICT COURT'S CONSTRUCTION OF USAGE RIGHTS SHOULD BE AFFIRMED. 36

A. The Patents Require That Usage Rights Be Attached to Digital Works. 36

B. The Court's Construction Properly Captures The Required Relationship Between Usage Rights and Content. 38

C. The District Court Properly Held the Parties to Its Claim Construction. 42

D. Prosecution Disclaimer and Judicial Estoppel Bar ContentGuard From Challenging the Construction of "Usage Rights." 47

III. THIS COURT SHOULD AFFIRM THE JUDGMENT OF NONINFRINGEMENT. 50

A. Modification of a Claim Construction Does Not Require a New Trial Where Other Claim Limitations Are Not Met. 51

B. Apple's Accused Systems Do Not Meet Unchallenged Portions of the Construction of "Usage Rights." 52

C. Apple's Accused Systems Do Not Meet the "Repository" Limitations. 55

1. The Devices that Make Up Apple's System Do Not Maintain the Required Integrities. 55

2. The Construction of Usage Rights Has No Bearing on ContentGuard's Failure of Proof Regarding the Repository Limitations. 61

D. Apple's JMOL Opposition Is Irrelevant. 62

IV. CONTENTGUARD IS NOT ENTITLED TO A NEW TRIAL BASED ON THE DISTRICT COURT'S EVIDENTIARY RULINGS. 64

A. ContentGuard Fails Even To Argue That Any Particular Ruling Was An Abuse of Discretion That Affected Its Substantial Rights. 64

B. ContentGuard's Source Code Complaints Fail Because The Court Granted the Relief ContentGuard Sought and Other Evidence Unequivocally Established Macs and PCs are Not Repositories. 65

C. ContentGuard's "rsync" Complaints Rest on a Legally Flawed Infringement Theory and Distortions of the Record. 67

1. ContentGuard Cannot Prove Behavioral Integrity Based on Secure Communication Protocols. 68

2. ContentGuard's "rsync" Complaints are Meritless. 72

V. THE ASSERTED CLAIMS ARE UNPATENTABLE UNDER § 101 AND INVALID UNDER § 103. 75

A. ContentGuard's Patents Are Drawn to Unpatentable Subject Matter. 75

1. The Asserted Stefik Claims Are Not Patent Eligible. . 76

2. Claim 1 of the '053 Patent Fails to Recite Patent-Eligible Subject Matter. 77

B. The Prior Art Presented at Trial Established That The Stefik Patent Claims Are Obvious. 78

1. The Combination of ABYSS and Dyad Discloses Both Repositories and Usage Rights. 79

2. ContentGuard Failed To Rebut The Substantial Evidence of Invalidity. 81

C. The Asserted Claims Of The '053 Meta-Rights Patent Are Invalid As Obvious Based On The Stefik '980 Patent. 82

1. The '053 Patent Acknowledges Stefik '980 As Prior Art and Adds No Non-Obvious Additional Limitations. 83

2. The Stefik '980 Patent Discloses Or Makes Obvious Every Limitation Of Claim 1 Of The '053 Patent. 84

D. Apple Is Entitled in the Alternative to a New Trial on Invalidity. 91

VI. CONCLUSION 92

TABLE OF AUTHORITIES

Page(s)

Cases

Alice Corp. Pty. v. CLS Bank Int'l,
134 S. Ct. 2347 (2014) 76

Allergan, Inc. v. Athena Cosmetics, Inc.,
640 F.3d 1377 (Fed. Cir. 2011) 35

ArcelorMittal v. AK Steel,
700 F.3d 1314 (Fed. Cir. 2012) 40

Atlas IP, LLC v. Medtronic, Inc.,
809 F.3d 599 (Fed. Cir. 2015) 4

Bosarge v. Mississippi Bureau of Narcotics,
796 F.3d 435 (5th Cir. 2015) 35

Cambridge Toxicology Grp., Inc. v. Exnicios,
495 F.3d 169 (5th Cir. 2007) 35

Cardiac Pacemakers, Inc. v. St. Jude Med., Inc.,
576 F.3d 1348 (Fed. Cir. 2009) (en banc) 92

Clay v. United States,
537 U.S. 522 (2003) 3

Cole v. Kimberly-Clark Corp.,
102 F.3d 524 (Fed. Cir. 1996) 49

In re Comiskey,
554 F.3d 967 (Fed. Cir. 2009) 77

Computer Docking Station Corp. v. Dell, Inc.,
519 F.3d 1366 (Fed. Cir. 2008) 49, 58

Dieser v. Cont'l Cas. Co.,
440 F.3d 920 (8th Cir. 2006) 4

EEOC v. Manville Sales Corp.,
27 F.3d 1089 (5th Cir. 1994) 35

FirsTier Mortgage Co. v. Investors Mortgage Ins. Co.,
498 U.S. 269 (1991) 5

Geo. M. Martin Co. v. All. Mach. Sys. Int'l LLC,
618 F.3d 1294 (Fed. Cir. 2010) 82

Google Inc. v. ContentGuard Holdings, Inc.,
CBM2015-00040, 2016 WL 3438922 (PTAB June 21, 2016) 47

GPNE Corp. v. Apple Inc.,
830 F.3d 1365 (Fed. Cir. 2016) 38

Intellectual Ventures I LLC v. Symantec Corp.,
838 F.3d 1307 (Fed. Cir. 2016) 77

In re Jack Raley Constr., Inc.,
17 F.3d 291 (9th Cir. 1994) 5

Jonsson v. Stanley Works,
903 F.2d 812 (Fed. Cir. 1990) 50

In re Keller,
642 F.2d 413 (C.C.P.A. 1981) 81

Marandola v. United States,
518 F.3d 913 (Fed. Cir. 2008) 6

Microsoft Corp. v. Multi-Tech Sys., Inc.,
357 F.3d 1340 (Fed. Cir. 2004) 49

New Hampshire v. Maine,
532 U.S. 742 (2001) 50

Nuance Commc'ns, Inc. v. ABBYY USA Software House, Inc.,
813 F.3d 1368 (Fed. Cir. 2016) 52

OIP Techs., Inc. v. Amazon.com, Inc.,
788 F.3d 1359 (Fed. Cir. 2015) 35

Ormco Corp. v. Align Tech., Inc.,
463 F.3d 1299 (Fed. Cir. 2006) 82

PPG Indus., Inc. v. Celanese Polymer Specialties Co.,
840 F.2d 1565 (Fed. Cir. 1988) 3

Pandrol USA, LP v. Airboss Ry. Prods., Inc.,
320 F.3d 1354 (Fed. Cir. 2003) 4

Poly-America, L.P. v. API Indus., Inc.
No. 2016-1200, – F.3d –, 2016 WL 5956745 (Fed. Cir. Oct. 14, 2016) 39

Quackenbush v. Allstate Ins. Co.,
517 U.S. 706 (1996) 3

Rissetto v. Plumbers and Steamfitters Local 343,
94 F.3d 597 (9th Cir. 1996) 50

Spectrum Intern., Inc. v. Sterilite Corp.,
164 F.3d 1372 (Fed. Cir. 1998) 49

SSL Servs., LLC v. Citrix Sys., Inc.,
769 F.3d 1073 (Fed. Cir. 2014) 34, 35, 51

Stoney Point Prods., Inc. v. Underwood,
15 Fed. App'x 828 (Fed. Cir. 2001) 5

Teleflex, Inc. v. Ficosa N. Am. Corp.,
299 F.3d 1313 (Fed. Cir. 2002) 35, 53

TiVo, Inc. v. Echostar Communs. Corp.,
516 F.3d 1290, 1311–12 (Fed. Cir. 2008) 46

Trs. of Columbia Univ. v. Symantec Corp.,
811 F.3d 1359 (Fed. Cir. 2016) 39

United States v. Carter,
953 F.2d 1449 (5th Cir. 1992) 65

United States v. Cooper,
135 F.3d 960 (5th Cir. 1998) 5

United States v. Potts,
644 F.3d 233 (5th Cir. 2011) 64

Vasudevan Software, Inc. v. MicroStrategy, Inc.,
782 F.3d 671 (Fed. Cir. 2015) 34, 41

Verizon Servs. Corp. v. Vonage Holdings Corp.,
503 F.3d 1295 (Fed. Cir. 2007) 39

Other Authorities

Fed. R. App. P. 4(a)(2) 5

11 Wright, Miller & Kane, *Federal Practice and Procedure*
§ 2805 (2016) 74

STATEMENT OF RELATED CASES

Pursuant to Fed. Cir. R. 47.5, Defendant–Cross-Appellant Apple Inc. states as follows:

Apple previously sought *mandamus* relief from this Court with respect to Apple's motion to transfer venue. Appx567. The relief requested by Apple was denied. *Id.*

The appeals from *ContentGuard Holdings, Inc. v. Google Inc., et al.*, No. 14-cv-0061 (E.D. Tex.), Nos. 2016-2430, 2016-2431, 2016-2445, 2016-2446, 2016-2447, and 2016-2448, are pending before this Court.

The appeals 2016-2548, 2016-2557, 2016-2629 (each captioned *Apple Inc. v. ContentGuard Holdings, Inc.*) and 2016-2559 (*Google Inc. v. ContentGuard Holdings, Inc.*) from USPTO post-grant review proceedings are pending before this Court, and involve a patent asserted by ContentGuard in the district court that was ultimately not included in the trial.

JURISDICTIONAL STATEMENT

ContentGuard's jurisdictional statement is incorrect. This Court lacks jurisdiction over ContentGuard's appeal (2016-1916).

ContentGuard's complaint alleged infringement by Apple of nine patents: U.S. Patent Nos. 6,963,859 ("'859 Patent"); 7,225,160 ("'160 Patent"); 7,269,576 ("'576 Patent"); 7,523,072 ("'072 Patent"); 7,774,280 ("'280 Patent"); 8,001,053 ("'053 Patent"); 8,393,007 ("'007 Patent"); 8,370,956 ("'956 Patent"); and 8,583,556 ("'556 Patent"). Appx3234-3325. ContentGuard later identified specific asserted claims from each patent. Appx3516-3519.

Apple denied infringement, and asserted defenses and counterclaims seeking declaratory judgments of noninfringement, invalidity, and unenforceability. Appx3344-3386. In June 2015, the district court dismissed all claims and counterclaims concerning the '556 and '160 Patents. Appx3391; Appx3392.

ContentGuard did not pursue the alleged infringement of the '576 and '280 Patents in the November 2015 trial; it pursued infringement of only one claim from each of the '053, '072, '859, '007, and '956 Patents. Appx3561-3563. Equitable issues, including Apple's unenforceability

counterclaims, were not tried to the jury. The jury found all five claims not infringed and not invalid. Appx2716-2718. The district court entered judgment on the verdict on November 24, 2015, and denied the parties' post-trial motions on April 18, 2016. Appx1-2; Appx161.

The post-trial motions did not address the '576 and '280 Patents which ContentGuard had not pursued at trial, or the other patent claims that ContentGuard had asserted but did not present to the jury. The court's orders likewise did not address those claims, or Apple's corresponding counterclaims.

The claims and counterclaims that therefore were still pending include:

(i) ContentGuard's claims that Apple infringed the '576 and '280 Patents and the asserted claims of the '053, '072, '859, '007, and '956 Patents not pursued at trial; and

(ii) Apple's counterclaims seeking declaratory judgments as to the '576 and '280 Patents (noninfringement, invalidity, and unenforceability) and the '053, '072, '859, '007, and '956 Patents (unenforceability).

The parties and the court knew that various claims and counterclaims remained unresolved. Apple had raised that issue in a February 2016 hearing on the post-trial motions. In particular, Apple had explained that its inequitable conduct counterclaim would need to be resolved and "put in a package so that a final judgment can be entered that disposes of the entire case for purposes of appeal." Appx3783(66:18-20). The court took no action on the unresolved claims, but instead suggested that the parties attempt to agree upon a proposed resolution. Appx3783-3784(66:12-67:3). No such resolution had been reached or adopted by the court as of April 22, 2016, when ContentGuard filed its notice of appeal. Because claims and counterclaims remained unresolved, there was no final and appealable judgment at that point. *Clay v. United States*, 537 U.S. 522, 527 (2003) ("[A] federal judgment becomes final for appellate review … when the district court disassociates itself from the case, leaving nothing to be done at the court of first instance save execution of the judgment."); *Quackenbush v. Allstate Ins. Co.*, 517 U.S. 706, 712 (1996) (same); *PPG Indus., Inc. v. Celanese Polymer Specialties Co.*, 840 F.2d 1565, 1567 (Fed. Cir. 1988) (same).

On April 28, 2016, about one week after ContentGuard filed its notice of appeal, Apple filed an agreed motion proposing that the court dismiss the still-pending claims and counterclaims, variously with and without prejudice, Appx3786-3790, which the court granted on May 2, 2016, Appx3791-3792. Only then did the judgment become final and appealable because only then had all claims and counterclaims been resolved. *See Pandrol USA, LP v. Airboss Ry. Prods., Inc.*, 320 F.3d 1354, 1362 (Fed. Cir. 2003) ("If a case is not fully adjudicated as to all claims for all parties, there is no final decision and therefore no jurisdiction…. A judgment that does not dispose of pending counterclaims is not a final judgment.") (citation and quotation marks omitted). *See also Atlas IP, LLC v. Medtronic, Inc.,* 809 F.3d 599, 604 (Fed. Cir. 2015) ("[A] final judgment exists when a district court fully adjudicates some claims and by consent dismisses all remaining counterclaims without prejudice.").

ContentGuard's April 22, 2016 notice of appeal is ineffective because the district court had not entered final judgment before ContentGuard filed it. *Dieser v. Cont'l Cas. Co.*, 440 F.3d 920, 926-27 (8th Cir. 2006) (notice of appeal ineffective where litigation was non-

final), citing, *inter alia*, *Stoney Point Prods., Inc. v. Underwood*, 15 Fed. App'x 828, 830-31 (Fed. Cir. 2001) (unpub.); *In re Jack Raley Constr., Inc.*, 17 F.3d 291, 294 (9th Cir. 1994) (dismissing for lack of jurisdiction where notice of appeal was premature). *See also United States v. Cooper*, 135 F.3d 960, 963 (5th Cir. 1998) (reaching same result under FRAP 4(b) in a criminal case). [1]

FRAP 4(a)(2) provides a limited exception for prematurely filed notices of appeal, but that exception applies only where "a district court announces a decision that *would be* appealable if immediately followed by the entry of judgment." *FirsTier Mortgage Co. v. Investors Mortgage Ins. Co.*, 498 U.S. 269, 276 (1991). The court below had not announced any decision concerning the unresolved claims and counterclaims before ContentGuard filed its notice of appeal. Unlike the cases the Supreme Court highlighted from the Advisory Committee Note to the Rule (where district courts had dismissed entire complaints but failed to enter final judgments), *id.* at 273, there was no basis for ContentGuard

[1] Apple's May 10, 2016 Docketing Statement in this Court noted the "Nature of judgment" as "Other" rather than a final judgment, and explained that ContentGuard had filed its notice of appeal before entry of the district court's order dismissing the remaining claims and counterclaims. *See* Dkt. 14.

to believe that a final judgment existed on April 22, 2016, in view of (1) Apple's earlier statements that its inequitable conduct counterclaim would need to be resolved "so that a final judgment can be entered that disposes of the entire case for purposes of appeal," Appx3783(66:18-20); (2) Apple's filing of an *agreed* motion directed to the still-pending claims and counter-claims, Appx3786-3790; and (3) the court's granting of that motion on May 2, 2016, Appx3791-3792.

Because ContentGuard filed its notice of appeal before all claims and counterclaims had been resolved, and did not thereafter file another notice, this Court lacks jurisdiction over ContentGuard's appeal under FRAP 4(a)(1)(A). *Marandola v. United States*, 518 F.3d 913, 914 (Fed. Cir. 2008) ("An untimely appeal must be dismissed for lack of jurisdiction."), citing *Bowles v. Russell*, 551 U.S. 205 (2007).

This Court does have jurisdiction over Apple's appeal (2016-2007) pursuant to 28 U.S.C. § 1295(a)(1). Apple's notice of appeal was timely filed on May 5, 2016. Appx3793-3795.[2]

[2] If this Court concludes that ContentGuard's appeal should be dismissed for lack of jurisdiction, Apple will voluntarily dismiss its appeal.

COUNTERSTATEMENT OF ISSUES

1. Whether the district court's construction of the claim term "usage rights" was correct in light of the specification's clear statements that usage rights must be attached to digital content.

2. Whether the judgment of noninfringement should be affirmed regardless of the construction of "usage rights" because no reasonable jury could find that Apple's accused systems met unchallenged claim limitations.

3. Whether the district court abused its discretion in granting ContentGuard the relief it requested to resolve discovery disputes, but refusing to grant ContentGuard's subsequent mid-trial requests for additional relief it had never previously requested.

4. (Apple's Appeal) Whether the asserted patents are invalid as obvious or for failure to claim patent-eligible subject matter, or in the alternative whether Apple is entitled to a new trial on invalidity.

COUNTERSTATEMENT OF THE CASE

I. INTRODUCTION

ContentGuard began as a spin-off from Xerox Corporation in the late 1990s, taking with it certain patent applications originally filed by Xerox in 1994. Appx1328-1329. Between then and 2013, ContentGuard

filed dozens of continuing applications, including six that later issued as patents asserted in this case.

ContentGuard's patents describe and claim an already-existing, impractical "trusted systems" approach to digital rights management ("DRM") that requires two key elements: (1) usage rights are attached to content, and (2) the content remains within a network of "repositories" that regulate its use and enforce those usage rights. Despite investments from Microsoft, Time Warner, and Technicolor, ContentGuard failed to commercialize its DRM technology, and currently makes no DRM products. Appx1330; Appx1349.

ContentGuard sued Apple (and others) in late 2013 for infringing ContentGuard's DRM patents. Appx502. ContentGuard's claims against Google and Samsung proceeded to trial in September 2015. The jury found that the accused Google Play Store (which sells digital books and movies) does not infringe. Appx3542-3543.

ContentGuard's claims against Apple were tried in November 2015. ContentGuard accused Apple's iTunes system (which Apple uses to distribute digital music, movies, and books) of infringing its patents, and initially sought nearly $1.5 billion in damages. Appx4722. By the

time of trial (and faced with multiple *Daubert* challenges), ContentGuard's demand dropped to $882 million. Appx1709(69:13-17). The jury found that Apple infringes none of the five claims pursued at trial. Appx2717.

On appeal, ContentGuard raises a single legal issue: whether one portion of the district court's construction of the claim term "usage rights" was incorrect. It was not. As the district court held, the specification of ContentGuard's patents compels the conclusion that usage rights must be attached to content. Indeed, ContentGuard itself assured the USPTO—in an attempt to rescue one of its patents from a Covered Business Method Patent Review—that the court's construction of "usage rights" is correct. ContentGuard concedes that if the court's construction of usage rights is correct—and it is—the noninfringement judgment must stand.

ContentGuard also raises discovery and evidentiary disputes, asserting that the district court abused its discretion in resolving them. But in the two instances complained of, ContentGuard asked the court for specific relief, and obtained the precise relief it sought. Neither provides any basis to disturb the jury's verdict.

ContentGuard's patents also fail to claim patent-eligible subject matter, particularly under the broader claim construction ContentGuard seeks. ContentGuard's claims merely describe in "digital" terms the same restrictions on loaning physical videotapes and books imposed by video rental stores (for decades) and libraries (for centuries). ContentGuard's patents are also invalid as obvious based on DRM systems that ContentGuard's inventors acknowledged as prior art.

The jury's verdict of non-infringement should be affirmed. If it is not, ContentGuard's claims should be held invalid.

II. STATEMENT OF FACTS

A. Digital Rights Management.

Digital rights management systems limit, control, or restrict what a user can do with a digital work (*i.e.*, a movie or book). For example, DRM technology may control whether a user can make a copy of the work, or whether the user can give the work to a friend.

ContentGuard's patents describe different prior art approaches to DRM, including two of particular relevance here: "secure containers and trusted systems." Appx373(1:57-58). A "secure container" is "simply an encrypted document," and provides DRM by "keep[ing] document

contents encrypted until a set of authorization conditions are met." Appx373(1:58-61). By contrast, in the "trusted systems" approach, "the entire system is responsible for preventing unauthorized use and distribution of the document," and digital works are kept within the trusted system. Appx373(2:4-6).

Building a trusted system for DRM "usually entails introducing new hardware such as a secure processor, secure storage, and secure rendering devices" and "requires that all software applications that run on trusted systems be certified to be trusted." Appx373(2:6-9).

B. ContentGuard's Trusted Systems Patents.

ContentGuard's patents criticize prior art DRM systems that use "secure containers," explaining that such systems cannot effectively control the use of content after it has been delivered and decrypted.[3] Once that happens, the content's use or transfer can no longer be controlled and it can be distributed for free. Appx192(6:22-28) ("[T]he content genie is out of the bottle."). ContentGuard's patents instead embrace a "trusted systems" approach that restricts transfer and use of

[3] One prior art DRM system specifically criticized by the patents was the license-server system described in a patent to Griswold that could be implemented entirely in software, but required continuous connection to a communications facility. Appx190(2:6-39).

content to "repositories" that enforce rules ("usage rights") that travel with each item of content. As each of ContentGuard's '072, '859, '007, and '956 patents (the "Stefik patents," all of which have expired) explains, the ContentGuard DRM system solves the problems with prior art systems by using a "combination of attached usage rights and repositories." Appx192(6:22-23).[4] The patents emphasize that these two features—repositories and attached usage rights—are key to ContentGuard's purported invention. Appx192(6:11-21).

1. Repositories.

In ContentGuard's patented system, digital content is passed *only* among devices that are repositories. Appx195(11:51-12:50). ContentGuard's system protects digital content by confining it to this end-to-end system of repositories. Even end-user devices must be repositories.

The district court (in constructions ContentGuard does not challenge) construed "repositories" to be devices that maintain three "integrities" in the support of usage rights—"physical integrity," "communications integrity," and "behavioral integrity." Appx18-23;

[4] The four Stefik patents have a common specification. Citations in this brief are to the specification of the '859 patent. Appx173-217.

Appx195(11:62-12:50). These "integrities" are *not* attributes of ordinary computers. As both the patents and Xerox engineers explained at the time, ordinary computers like Macs and PCs are not trusted systems, and cannot easily be modified to be trusted systems. Appx373(2:14-19); Appx967(8:17-23); Appx3922-3923; Appx979-982(20:16-23:15); Appx2158-2161(24:18-27:16); Appx2850-2852.

The court's claim construction lays out the specific integrity requirements for repositories, which are required in all claims, Appx13, Appx101:

- "Physical integrity" requires "preventing access to information in a repository by a non-trusted system." Appx20.
- "Communications integrity" requires that each repository "only communicates with other devices that are able to present proof that they are trusted systems." Appx20-21.
- "Behavioral integrity" requires "software to include a digital certificate in order to be installed in the repository."[5] Appx23.

[5] A "digital certificate" is a "signed digital message that attests to the identity of the possessor." Appx55. A digital certificate can be included in a piece of software, attesting to the identity of the manufacturer of that software. *See* Appx2187-2188.

Each of these integrities is a separate requirement. If a device maintains two, but not the third, it is not a "repository."

The court's construction also requires that a "repository" maintain all three of these integrities "in the support of usage rights." Appx17. While the precise contours of "in the support of usage rights" were largely not at issue at trial, operations involving the transfer of digital content, restricting access to content, or updates to alleged repository software are all circumstances in which the three integrities must be maintained. Appx1117-1118(158:15-159:11); Appx2204(70:7-17).

2. The Communications Integrity Requirement.

Under the claim construction that ContentGuard proposed and the court accepted, Appx20-21, repositories can communicate in the support of usage rights only with other repositories, so *all* devices participating in an allegedly-infringing DRM system must be repositories, and all must observe the three integrities when taking actions involving a digital work (*e.g.*, transferring it to another device).

A server in a DRM system might observe behavioral and physical integrity. But if as part of the process of transferring content, that server communicates with a device that does *not* meet all three

repository requirements, then that server also is *not* a repository, because it has communicated in the support of usage rights with a non-repository. This failure of that one server to maintain communications integrity in the support of usage rights infects the entire DRM system. That is, all of the other servers and devices in the system that transfer or use content also fail the communications integrity requirement, because they communicate with this "non-repository" server.

This consequence of a single point of failure makes sense in light of the systems described by the patents—communications integrity is necessary "in a world known to contain active adversaries." Appx195(12:32-33). If even one door is left ajar, an "active adversary" can get in and compromise not just one computer but the entire system.

Because of the communications integrity requirement, there cannot be infringement with respect to *some* parts of a DRM network like Apple's iTunes/FairPlay system and not others. A system that allows transfers to or use of content by even one non-repository cannot infringe ContentGuard's patents. ContentGuard therefore had to prove that all of the servers, computers, and devices that transfer or use content in Apple's system are repositories. The failure of even one

component to maintain the three integrities while transferring or using content means that the Apple system as a whole does not infringe.

3. Usage Rights.

Usage rights are "rights granted to a recipient of a digital work," which "define how a digital work can be used and if it can be further distributed." Appx192(6:3-8). Repositories enforce usage rights "to determine what transactions can be successfully carried out for a digital work." Appx197-198(16:64-17:3). For example, usage rights "determine whether a digital work can be copied, when and how it can be used," and so on. Appx198(17:3-6). The patents describe various types of usage rights, including basic rights like Play, Print, Copy, Transfer, Loan, Appx198-199(18:44-19:4), and complex rules for tracking copy counts and metering usage fees, Appx199-201(20:9-24:10). *See also* Appx201-202(24:11-25:36) (examples of usage rights).

In ContentGuard's claimed system, usage rights are attached to digital content. Appx194-195(10:44-11:2). The patents' specification is adamant throughout that usage rights and content *must* stay together—as the patents explain, by requiring attachment, "the usage rights and any associated fees assigned by a creator and subsequent

distributor *will always remain with a digital work*." Appx192(6:13-16). Likewise, when explaining how the claimed systems execute a "Usage Transaction"—for example, a request to view a digital work—a repository must determine if the conditions dictated by the usage rights are satisfied. Appx204-205(29:36-31:42); Appx188.

The patents thus make clear that the combination of attached usage rights and repositories is critical to their purported invention. If the usage rights are not attached to the digital work, the repository would have nothing to check and no way to determine whether a particular transaction is authorized. *See id*. That would allow the content to escape regulation by the system and to be transferred or used in violation of the rules defined in the usage rights. That is why the specification emphasizes that "[a] key feature of the present invention is that usage rights are permanently 'attached' to the digital work." Appx192(6:11-12).

The use of repositories in combination with attached usage rights also solves the recognized problem of the "secure container" approach's reliance on encryption. Specifically, because the Stefik system restricts the movement and use of content only to repositories, and because those

repositories must enforce the usage rights that are always with the content, the Stefik approach eliminates the risk that content, after being decrypted, will escape—the content "genie" is thus always kept in the DRM "bottle."

4. ContentGuard's Meta-Rights Patent.

ContentGuard's '053 Patent—the fifth patent ContentGuard pursued at trial—purports to build on Stefik's alleged inventions by adding the concepts of "meta-rights" and "state variables." Appx375(5:19-59). An example of a meta-right is the right to grant usage rights—in other words, the right to sublicense. Appx108; Appx375(5:22-23); Appx1213(76:14-16). State variables are used to track the status of a usage right. Appx116. For example, a usage right might permit a user to print DRM-protected content three times; a state variable tracks how many times the content has been printed. Appx375(5:48-53). Like the Stefik patents, the '053 Patent requires use of repositories. Appx101.

C. Apple's iTunes/FairPlay System.

ContentGuard accused Apple's iTunes system of infringement. iTunes uses a DRM system called FairPlay to distribute content to

devices like iPhones, iPads, iPods, AppleTVs, and both Mac and PC computers running iTunes software. Appx1757-1760(117:9-120:16).

In contrast to the complex trusted systems approach to DRM claimed in ContentGuard's patents, FairPlay is an encryption-based "secure container" DRM system. Apple designed iTunes and FairPlay to provide a simple, flexible DRM system that customers can easily use. Appx1756-1757(116:11-118:10). FairPlay protects content by encrypting it and then carefully regulating how and when it can be decrypted. As in any secure container approach, once content is decrypted in the Apple system, it is at risk. FairPlay limits that risk by controlling which devices get the keys needed to decrypt and view the content, hiding where the keys are stored on a device, and decrypting only few frames of a movie or a few pages of a book at a time so that the entire work is never exposed. Appx1762(122:5-11); Appx1980-1981(3:10-4:3). By carefully regulating access to and use of the decryption keys, and by decrypting only portions of a work at a time, Apple's system addresses the "content genie out of the bottle" problem with the secure container encryption approach to DRM.

Apple's iTunes/FairPlay system does not use "repositories" with the three required "integrities." To the contrary, FairPlay can be used on many different kinds of devices, computers, and servers—including the Macs and PCs that ContentGuard's own patents acknowledge are not "repositories." Appx1758-1759(118:11-119:11); Appx373(2:14-19). All of these devices, computers, and servers play an interconnected role in transferring the content and keys that make FairPlay work.

Apple's system also does not employ "usage rights" that dictate what a user may or may not do with a piece of content. Instead, in Apple's system, digital content is distributed in encrypted form to devices or computers running iTunes (*i.e.*, iPhones, iPads, iPods, AppleTVs, Macs, and PCs). The content is sent to user devices from servers operated by a third party, Akamai, around the country. Appx1913-18. Apple servers independently distribute decryption keys, which the devices use to decrypt the content when a user wishes to play a movie or read a book. So, in Apple's system, the keys and content come from different places and do not travel together. Appx1763-1764(123:8-124:10). By regulating how and when these decryption keys

can be used, iTunes is able to protect the content and control its use.[6] Appx1912.

Apple intentionally designed FairPlay *not* to require repositories or complex "usage rights" as found in DRM systems like those claimed by Stefik. Steve Jobs and the engineers who designed FairPlay were aware of such systems, and decided not to follow that approach. Appx1764-1765(124:11-21); Appx1766-1770(126:5-130:3); Appx4526-4527 (Jobs email stating "Let's not use this DRM"). To that end, Apple's system does not allow movie studios or other content owners to set different usage rules for different pieces of content. All content in Apple's system follows the same, simple rule for all users: If a user's device has the correct keys, the device can decrypt the content and play it. Appx1764-1765(124:11-125:5) ("We didn't have to give every movie or every book its own set of usage rights. We simply had to control whether the user could view it … or read it by whether or not the key was present on their computer."). From inception, Apple did not want

[6] ContentGuard did not allege that the keys are "usage rights." Appx1105-1109(146:6-150:18). In related proceedings before the PTAB, ContentGuard affirmatively stated that decryption keys are not usage rights. *See* Prelim. Resp. of Patent Owner, Dkt. 10, IPR2015-00441 ('859 Patent) at 32 (Apr. 15, 2015).

to limit iTunes to repositories. For the iTunes Store to succeed, Apple needed to sell content to users who use Macs or PCs, devices over which the users (not Apple) have control. Appx1758-1759(118:11-119:11).

III. PROCEEDINGS BELOW

A. The Parties' Claims.

ContentGuard's complaint generally alleged that Apple's iTunes/FairPlay system infringed nine ContentGuard patents; ContentGuard subsequently identified specific asserted claims from each. Appx3234-3325; Appx3516-3519. Apple denied infringement, and asserted defenses and counterclaims seeking declaratory judgments of noninfringement, invalidity, and unenforceability as to each patent.

Along with other defendants, Apple moved for judgment on the pleadings that ContentGuard's patents claimed ineligible subject matter under Section 101, which the district court denied. Appx3548-3560.

B. Claim Construction.

On March 3, 2015, the district court entered a 144-page claim construction order construing more than 50 terms across the asserted claims of ContentGuard's nine patents. Appx4-5. As relevant here, the court adopted ContentGuard's proposed constructions for "repository,"

"communications integrity," and "behavioral integrity." Appx12-23. The court's construction of "physical integrity" differed slightly from ContentGuard's proposal, but ContentGuard does not challenge it on appeal. Appx18-20.

ContentGuard proposed that the court construe "usage rights" to mean:

> an indication of the manner in which a [digital work / digital content / content / a digital document] may be used or distributed as well as any conditions on which use or distribution is premised.

Appx25. In light of the unequivocal statement in the specification that "[a] key feature of the present invention is that usage rights are permanently 'attached' to the digital work," and the specification's repeated insistence that "usage rights" must be attached to content, Apple urged that the court include the requirement that "Usage rights must be permanently attached to the digital work." Appx25. The court declined to require permanent attachment, but added the bolded phrase to ContentGuard's language:

> indications **that are attached, or treated as attached, to [a digital work / digital content / content / a digital document] and that** indicate the manner in which the [digital work / digital content / content / digital document] may

> be used or distributed as well as any conditions on which use or distribution is premised.

Appx35.

C. Discovery Disputes.

1. ContentGuard's Source Code Production Complaints.

Apple produced extensive source code for its iTunes/FairPlay system during discovery. Although ContentGuard raised various complaints about Apple's production, the parties and the court eventually agreed in November 2014 that if ContentGuard had difficulties determining how Apple's produced source code worked, ContentGuard could request a deposition of a knowledgeable Apple engineer. Appx3428-3429; Appx3434-3437. ContentGuard never did.

Instead, ContentGuard waited and re-raised the source code dispute in *Daubert* briefing in June 2015. ContentGuard sought to exclude certain paragraphs of the report of Apple's noninfringement expert, Dr. Kelly, which described tests demonstrating that Macs and PCs are not repositories. Appx3408-3410. ContentGuard claimed it could not rebut Dr. Kelly's analysis because ContentGuard was confused about Apple's source code for iTunes on Macs and PCs. *Id.* Although Apple disagreed, the court excluded the paragraphs of Dr.

Kelly's report that ContentGuard attacked. Appx578. ContentGuard did not seek any other relief.

2. Discovery Concerning Updates to FairPlay Servers.

The court's unchallenged construction of "behavioral integrity" requires that software installed in a repository "include a digital certificate." Appx23. Accordingly, ContentGuard took discovery about the software updates installed on Apple's FairPlay servers, one of the many devices it needed to prove are repositories. Apple's witness testified that although the FairPlay servers previously used a single shared file system for software updates, there are now approximately 250 servers, each of which gets its own "local" copy of the software update. Appx3615(59:13-61:21). He testified that Apple system administrators manage this update process. *Id*. ContentGuard did not ask him to identify the particular utility Apple personnel use to copy files to the servers, likely because given the court's claim construction, the copying process is irrelevant; it could not affect whether the software update itself included a digital certificate, as the claim construction requires.

Eight months before trial, another Apple engineer in his deposition identified "rsync" as a utility used to copy certain files onto other servers, including files involved in the iTunes/FairPlay system. Appx3673(139:18-19). Rsync is an open source file transfer utility that runs on a variety of operating systems, with source code publicly available online.[7] *See* Appx2104(115:16-17) ("rsync is a UNIX command that has been around 30 or more years."). Despite being told that Apple used rsync in connection with FairPlay file transfer processes, ContentGuard did not seek additional discovery concerning rsync or claim that Apple's production regarding rsync was insufficient.

D. Trial and Jury Verdict.

As noted above, at trial ContentGuard pursued alleged infringement of only one asserted claim from each of the '053, '072, '859, '007, and '956 Patents. Apple presented its corresponding invalidity defenses and counterclaims.

1. The District Court Resolves the rsync Issue.

By the time of trial, ContentGuard's "behavioral integrity" infringement theory had shifted. Although the claim construction

[7] *See* https://rsync.samba.org/.

requires software to "include a digital certificate," Appx23, discovery confirmed that Apple's server software updates do not include such certificates.

ContentGuard thus concocted a theory under which the method Apple uses to transfer software updates to its servers somehow met the "behavioral integrity" requirement, even though the software updates themselves did not include the required digital certificate. Specifically, ContentGuard argued that a secure communications channel (which may be established using a digital certificate) could fulfill the requirement that the *software* itself include a digital certificate. Because that theory collapsed the requirement that a repository maintain communications integrity (which requires data to be sent over a secure channel) with the requirement that the repository exhibit behavioral integrity (which requires software to include a digital certificate), ContentGuard effectively argued that a system with communications integrity would necessarily also have behavioral integrity.

To that end, ContentGuard asked at trial how software updates are moved to Apple's servers. Apple's witness accurately (and

consistent with his prior testimony) identified the rsync utility as the tool used to do that. Appx2102-2103(113:23-114:1). ContentGuard then seized on that response as a startling new revelation of previously-hidden information material to its infringement case.

Although ContentGuard on appeal tries to create the impression that the district court ignored its (unfounded) complaints, the court provided a remedy, which ContentGuard accepted without objection. Specifically, ContentGuard was permitted to offer—in its rebuttal case, and over Apple's objection—additional infringement testimony outside its expert reports concerning Apple's use of rsync. *See* Appx2326(60:7-9); Appx2483-2486(47:11-50:9). ContentGuard never made any further objection, nor did it argue that it was entitled to additional relief. *See* Appx2424(158:18-21); Appx2440-2441(4:8-5:8).

2. The Jury Finds Apple Does Not Infringe.

The jury found that Apple does not infringe, and there were multiple grounds on which that finding could have rested. Under the court's construction of "usage rights," ContentGuard was required to prove that Apple's accused system employed rights that "indicate the manner in which" a digital work "may be used or distributed as well as

any conditions on which use or distribution is premised," and that these rights are "attached, or treated as attached" to content. Appx35. As to the latter requirement, ContentGuard's expert pointed to a variety of supposed connections between what he said were Apple's "usage rights" and the content, including ID numbers, memory addresses, pointers and links, and the like, Appx1052-1054(93:3-95:23); Appx1110-1112(151:20-153:4); Appx1147(10:11-22), all of which he said established that Apple's system has usage rights that are attached or treated as attached to content. On appeal, ContentGuard does not argue that this testimony or any of its other evidence compelled a finding that Apple's supposed usage rights were "attached, or treated as attached" to content. Therefore, if that portion of the construction is correct, ContentGuard concedes that the noninfringement verdict should stand.

ContentGuard also does not argue that the evidence at trial established the other component of the "usage rights" construction — that Apple's system include rights that define how a work can be used. The evidence, in fact, established that Apple's system does not employ such "usage rights." And that is so regardless whether the items

ContentGuard identified as Apple's alleged "usage rights"—the "kind" and "isRental" data fields contained in a "Purchase Response" message transmitted within Apple's iTunes system, Appx1105-1106(146:6-147:9)—are attached or treated as attached to content. Unrebutted testimony confirmed that these data fields play no role in enforcing how digital content is used by iTunes customers, which ContentGuard experts acknowledged usage rights must do. Appx1178(41:22-24).

Beyond "usage rights," ContentGuard also had to prove that each of the devices, computers, and servers in the iTunes/FairPlay system is a repository in connection with the transfer and use of DRM-protected content. That is because the unchallenged construction of "communications integrity" requires that every repository communicate only with other repositories when taking actions in the support of usage rights. Appx20-21. ContentGuard failed to carry that burden.

In particular, ContentGuard offered no evidence that Apple's servers, which deliver the decryption and user keys to user devices, are repositories. ContentGuard did not present evidence that those servers have "behavioral integrity," and they do not because they do not require

that software include a digital certificate in order to be installed. There is no contrary evidence.

ContentGuard also offered no evidence that most of the devices that receive content in the Apple system are repositories. ContentGuard focused only on the iPad, and did not present evidence that the iPad is representative of all other devices in the Apple system—there was substantial evidence that it is not.[8] In any event, the evidence showed even the iPad is not a repository. Appx1954-55(116:13-117:1); Appx2196-2200(62:17-66:11); Appx2293-2294(27:23-28:11).

SUMMARY OF ARGUMENT

As a threshold matter, ContentGuard's appeal should be dismissed for lack of jurisdiction. ContentGuard filed its notice of

[8] ContentGuard admits it "presented its infringement proof using the iOS code that runs on Apple's iPhones and iPads, and ContentGuard's experts treated the Mac and PC versions of the iTunes code as being the same as that running on the iOS products." (Br. 25.) ContentGuard suggests that it was "[w]ithout access to the Mac and PC versions of the iTunes software," but that is false—it had access to the software, but only later in the case claimed it lacked access to additional "correlation folders," which were created by Apple specifically for this litigation to assist ContentGuard's review of Apple's code. Appx4752. As noted above (p. 25), ContentGuard never took the deposition it had been granted months earlier to resolve any concerns about its "access to the Mac and PC versions of the iTunes software."

appeal before a final and appealable judgment had been entered, and failed to file a notice of appeal after such a judgment existed. The district court had not announced any decision on the unresolved claims before entering that judgment, so the narrow exception in FRAP 4(a)(2) does not apply. This Court lacks jurisdiction over ContentGuard's appeal.

On the merits, the district court's construction of "usage rights" should be affirmed. The asserted patents repeatedly insist that usage rights must be attached to digital content, fully supporting the construction's requirement that usage rights are "attached, or treated as attached to content." ContentGuard's own representations to the PTAB, urging it to adopt the same construction of "usage rights," cement the conclusion that this construction is correct. ContentGuard does not dispute that it failed to prove infringement under that construction, and so the judgment should be affirmed.

Entirely apart from the "attached, or treated as attached" portion of the construction of "usage rights," the judgment should be affirmed, because Apple's accused system does not meet other, *unchallenged* portions of the construction. First, Apple's system does not have "usage

rights" even under the construction ContentGuard now seeks, and no reasonable jury could have found that it does. Apple's accused system also does not meet the "repository" limitations of the claims because it is undisputed that devices without behavioral or communications integrity transfer and use content in Apple's system. Thus, ContentGuard cannot show infringement even under the construction of "usage rights" it seeks on appeal, so it is not entitled to a new trial under any circumstances.

The remainder of ContentGuard's appeal consists of complaints about two discovery disputes. ContentGuard's arguments concerning those disputes are without merit, and neither provides a basis to disturb the verdict, because in both instances, ContentGuard sought specific relief from the district court, *which the court granted*. Those rulings in ContentGuard's favor cannot possibly be an abuse of discretion.

If, notwithstanding all of this, the Court were to consider ContentGuard's pleas for relief from the judgment—including the broadened claim construction it seeks—the Court would also need to address the unpatentability of ContentGuard's claims under Section

101 and invalidity under Section 103. ContentGuard's patents claim nothing more than the "library loan" concept for the digital world, and add nothing inventive to that abstract concept. Further, DRM systems that used "trusted systems" in combination with usage rights associated with digital content were known well before ContentGuard's patents, and the particular recitations in the ContentGuard claims are at best obvious combinations of those prior art concepts.

ARGUMENT

I. STANDARD OF REVIEW

This Court "review[s] de novo the ultimate question of the proper construction of patent claims and the evidence intrinsic to the patent." *Vasudevan Software, Inc. v. MicroStrategy, Inc.*, 782 F.3d 671, 676 (Fed. Cir. 2015). Subsidiary factual findings underlying a district court's claim construction are reviewed for clear error. *Id.*

Rulings on motions for a new trial, evidentiary issues, and discovery issues are reviewed for abuse of discretion under the law of the Fifth Circuit, the regional circuit here. *See SSL Servs., LLC v. Citrix Sys., Inc.*, 769 F.3d 1073, 1082 (Fed. Cir. 2014). Any error in the admission or exclusion of evidence "should not be the basis for setting aside the judgment" unless "substantial rights of the parties were

affected." *EEOC v. Manville Sales Corp.*, 27 F.3d 1089, 1093 (5th Cir. 1994).

The district court's denial of judgment on the pleadings is also reviewed under Fifth Circuit law, *Allergan, Inc. v. Athena Cosmetics, Inc.*, 640 F.3d 1377, 1380 (Fed. Cir. 2011), and is thus reviewed *de novo*, *Bosarge v. Mississippi Bureau of Narcotics*, 796 F.3d 435, 439 (5th Cir. 2015). Patent eligibility under Section 101 is also reviewed *de novo*. *See OIP Techs., Inc. v. Amazon.com, Inc.*, 788 F.3d 1359, 1362 (Fed. Cir. 2015).

The jury verdict is reviewed for substantial evidence. *Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1322-23 (Fed. Cir. 2002). The district court's denial of a motion for JMOL is reviewed *de novo,* applying the same standard as the district court. *SSL Servs.*, 769 F.3d at 1082. In the Fifth Circuit, JMOL "is appropriate only when a reasonable jury would not have a legally sufficient evidentiary basis to find for the party on that issue." *Cambridge Toxicology Grp., Inc. v. Exnicios*, 495 F.3d 169, 179 (5th Cir. 2007) (quotation marks omitted).

II. THE DISTRICT COURT'S CONSTRUCTION OF USAGE RIGHTS SHOULD BE AFFIRMED.

A. The Patents Require That Usage Rights Be Attached to Digital Works.

In ContentGuard's system, as digital content travels throughout a network of repositories, its movement and use are controlled by "usage rights" that dictate how that content may be transferred or used. *See* Appx198(18:13-17). As the specification explains, in prior systems digital content could be used on ordinary devices, where once it was decrypted it could no longer be controlled and could be freely distributed. Appx192(6:27-28).

The patents purport to solve that problem by ensuring that usage rights and content stay together:

> A key feature of the present invention is that usage rights are permanently "attached" to the digital work. Copies made of a digital work will also have usage rights attached. Thus, the usage rights and any associated fees assigned by a creator and subsequent distributor will always remain with a digital work.

Appx192(6:11-16).

The specification contains a section entitled "Attaching Usage Rights to a Digital Work," which explains, "[i]t is fundamental to the present invention that the usage rights are treated as part of the digital

work." Appx194(10:45-46). The specification makes clear that "[u]sage rights are attached directly to digital works," Appx193(8:33), and that "[t]he combination of attached usage rights and repositories enable distinct advantages over prior systems," Appx192(6:22-23).

The patents' Glossary definitions of "digital work" and "composite digital work" further confirm that usage rights must be "attached" to a digital work. Appx214(50:11-12) ("Usage rights and fees are attached to the digital work."); Appx214(49:49-51) ("Each of the distinguishable parts is itself a digital work which have usage rights attached.").

Additional, unequivocal descriptions requiring usage rights to be attached to content are found throughout the specification. *See, e.g.*, Appx177(Fig.1) ("Usage Rights Attached to Digital Work"); Appx191(3:49-51) ("It would be desirable to have a distribution system where the means for billing is always transported with the work."); Appx192(6:28-29) ("In contrast, the present invention never separates the fee descriptions from the work."); Appx192(6:36-38) ("The creator will then determine appropriate usage rights and fees, attach them to the digital work, and store them…"); Appx192(6:54-57) ("The check of the usage rights essentially involves a determination of whether a right

associated with the access request has been attached to the digital work…").

B. The Court's Construction Properly Captures The Required Relationship Between Usage Rights and Content.

Consistent with the patents' explanation that attachment of usage rights to content is "fundamental," the district court construed "usage rights" as:

> indications that are attached, or treated as attached, to [a digital work / digital content / content / a digital document] and that indicate the manner in which the [digital work / digital content / content / digital document] may be used or distributed as well as any conditions on which use or distribution is premised.

Appx35. The only addition the court made to the construction proposed by ContentGuard is the statement that the indications "are attached, or treated as attached" to the content. Appx25.

The "attached, or treated as attached" requirement reflects the specification's repeated statements that usage rights and content must be "attached" for the purported invention to work. *GPNE Corp. v. Apple Inc.*, 830 F.3d 1365, 1370 (Fed. Cir. 2016) ("When a patent 'repeatedly and consistently' characterizes a claim term in a particular way, it is proper to construe the claim term in accordance with that

characterization."); *Trs. of Columbia Univ. v. Symantec Corp.*, 811 F.3d 1359, 1363 (Fed. Cir. 2016) ("The only meaning that matters in claim construction is the meaning in the context of the patent.").

The specification's descriptions of attachment of usage rights to content as a "key feature of the present invention," Appx192(6:11-12), and as "fundamental to the present invention," Appx194(10:45-46), necessarily limit the scope of the invention. *See Verizon Servs. Corp. v. Vonage Holdings Corp.*, 503 F.3d 1295, 1308 (Fed. Cir. 2007) ("When a patent … describes the features of the 'present invention' as a whole, this description limits the scope of the invention."). Accordingly, the court properly rejected ContentGuard's attempt to eliminate any attachment requirement. *See Poly-America, L.P. v. API Indus., Inc.*, No. 2016-1200, – F.3d –, 2016 WL 5956745, *4 (Fed. Cir. Oct. 14, 2016) ("[A]n inventor may disavow claims lacking a particular feature when the specification describes 'the present invention' as having that feature.").

In addition to the clear statements in the specification, the court's *Markman* order cited to both the prosecution history and extrinsic evidence, including Stefik's writings, a declaration of ContentGuard's

expert, and deposition testimony of a prosecuting attorney. Appx32-34. The court noted Stefik's affirmation that his system required usage rights to be permanently attached to digital content. Appx33. In particular, the court cited Stefik's contemporaneous analogy, in other writings, of "attached usage rights" to tags on clothing: "Digital works come with tags on them. . . . [T]he tags are not removable." Appx4498. *See also* Appx4514 (tags on digital works "are permanently attached"). "[W]hen an inventor's understanding of a claim term is expressed in the prior art, it can be evidence of how those skilled in the art would have understood that term at the time of the invention." *ArcelorMittal v. AK Steel*, 700 F.3d 1314, 1321-22 (Fed. Cir. 2012).

ContentGuard ignores this evidence. Instead, ContentGuard offers an entirely new piece of extrinsic evidence—its unsuccessful RightsEdge product—and asserts that the court's construction is inconsistent with RightsEdge's operation. (Br. 30, 37; *see* Br. 16-19 (describing RightsEdge).) ContentGuard never raised that argument below and cannot raise it now. More fundamentally, any supposed inconsistency between the claim construction and RightsEdge is

irrelevant because ContentGuard cites no evidence that RightsEdge practiced the asserted claims. (*See* Br. 17-19, 37.)

The district court's conclusion that the extrinsic evidence presented in the *Markman* proceedings did not warrant "departing from the lexicography and descriptions of the invention in the specification, which support … requiring that usage rights are 'attached' to digital works," Appx35, was plainly correct and certainly not clearly erroneous. *See Vasudevan Software,* 782 F.3d at 676 ("[I]n considering extrinsic evidence, we review the subsidiary factual findings underlying the district court's claim construction for clear error.").

ContentGuard also points to portions of the specification describing how a "description tree" for usage rights could be stored separately from content. (Br. 35-36.) But the court properly found that the "description tree" contains "descriptions of usage rights rather than usage rights themselves." Appx32. Apart from that, it would not be inconsistent with the court's construction for usage rights and content to be stored in different portions of the same overall file structure, Appx193-4(8:46-9:25), and once content has been properly transferred to a repository, the content and usage rights components can be stored

in discrete physical components of that repository, Appx196(13:41-47); Appx184. Nothing in those passages contradicts the requirement that usage rights be "attached, or treated as attached" to content. Nor do they suggest that content can be transferred to or from a repository without its accompanying usage rights. To the contrary, the specification is clear that content and usage rights must remain together. Appx192(6:11-16); Appx192(6:28-29).

C. The District Court Properly Held the Parties to Its Claim Construction.

In an attempt to evade the unequivocal statements in the specification—including expressly definitional statements in the Glossary—that usage rights must be attached to content, ContentGuard seizes on the word "associated," found in some claims and a few spots in the specification. ContentGuard asserts that the district court erred because it concluded that "DRM systems that rely on usage rights that are 'associated with' content fall outside the scope" of the asserted claims (Br. 30) and "excluded a claimed embodiment" (Br. 33). ContentGuard is wrong.

First, the court did not hold that a system that relies on usage rights that are associated with content falls outside the claims, nor did

it exclude a claimed embodiment. Rather, the court, based on the claim language, specification, prosecution history, and extrinsic evidence, construed the claims to determine what *kind* of association they require, and properly concluded that the required association is one where usage rights are attached or treated as attached to content. The court did so fully aware of the claim language ContentGuard cites, including "associated with." Appx29. And the court did so pursuant to the parties' agreement that "usage rights" should receive the same construction in all of the asserted claims (Br. 32 n.4), both those that include the word "associated" and those that do not.[9] The court's construction properly captures the scope of all the asserted claims.

Second, ContentGuard never proposed a construction that used "associated with" to define the required connection between usage rights and content, instead proposing a construction that left that entirely unaddressed. Its complaint with Apple's proposed construction at the *Markman* stage was not that the construction failed to mention "associated," but that it required "*permanent* attachment." Appx28.

[9] Two asserted claims use the term "associated"; the three other claims (from three other patents) asserted at trial all contain the term "usage right[s]" but *not* the term "associated." *See* Appx305(51:43-62); Appx347(50:31-49); Appx382-383(20:44-21:5).

Indeed, in opposing Apple's construction, ContentGuard told the court that in ContentGuard's patents, "'attachment' is a metaphor to explain that rights should be associated with content, while 'permanent' attachment means that association persists for the term or life of the right." Appx29. Thus, ContentGuard's contention that the court's construction "excluded a claimed embodiment" is incorrect: usage rights that are attached or treated as attached to content (the court's construction) are, by ContentGuard's own reasoning, "usage rights *associated* with the content."

Indeed, in its brief in this Court in the Google-Samsung appeal, ContentGuard repeatedly states that "attachment" and "association" mean the same thing: "'attachment' is just another term for 'association,' as the specification and prosecution history both demonstrate. . .. 'Attachment' and 'association' thus mean one and the same thing in Dr. Stefik's patents." (Dkt. 43 in 16-2430 at 4.) These statements, along with the PTAB statement ContentGuard identifies (Br. 36-37; *see* Appx605 ("'associated with' and 'attached to' refer to the same relationship between usage rights and a digital work")) confirm that the district court's construction is correct. When the claims

describe "usage rights" as "associated" with a digital work, the claims must be construed, in light of the specification and the understanding of one of ordinary skill, to mean that "usage rights" are "attached or treated as attached" to content. As the PTAB explained, and as ContentGuard told the district court at the *Markman* stage and this Court in the Google-Samsung appeal, "associated" and "attached" describe the *same* requirement, not two different requirements.

Having construed the claims to require that usage rights be attached or treated as attached to content, the district court properly precluded ContentGuard's expert Dr. Goodrich from using the unconstrued term "association" to attempt to convey some other meaning. Appx154. Once claim language has been construed, it is the court's construction that governs, and allowing an expert to use unconstrued terms divorced from the court's construction undermines the *Markman* process and can only confuse and mislead the jury.

Moreover, in this case, the court's restriction on ContentGuard's expert amounted to nothing more than precluding him from using a single word—"associated"—in his testimony. Consistent with ContentGuard's view that "associated with" and "attached, or treated as

attached" describe the same relationship between content and usage rights, Dr. Goodrich was permitted to—and did—testify that the "attached, or treated as attached" requirement of the court's construction was satisfied by the same features that ContentGuard now says would have been covered by "associated with." (Br. 35.) Specifically, he testified that usage rights are attached or treated as attached as long as there are ID numbers, a memory address, a pointer or link, *etc.* Appx1052-1054(93:3-95:23); Appx1110-1112(151:20-153:4); Appx1147(10:11-22).

With the substance of its expert's testimony unimpeded, and with its concession that "associated" and "attached, or treated as attached" mean the same thing in these patents, ContentGuard's argument on appeal necessarily reduces to the proposition that its expert should have been permitted to use the term "associated" to suggest that the claim requirements could be satisfied by something other than what the court's construction required. That is wrong as a matter of law. *See, e.g., TiVo, Inc. v. Echostar Communs. Corp.*, 516 F.3d 1290, 1311–12 (Fed. Cir. 2008) ("Dr. Polish was allowed to testify regarding how the prior art related to the claims as construed. He was prohibited from

testifying about how the prior art related to 'Dr. Gibson's view of the claims.' … The court's ruling therefore did not deprive EchoStar of any evidence it was entitled to introduce; at the same time, the court's ruling avoided possible jury confusion by ensuring that the invalidity inquiry focused on the relationship between the prior art and the claims, as construed by the court.").

D. Prosecution Disclaimer and Judicial Estoppel Bar ContentGuard From Challenging the Construction of "Usage Rights."

While this case was pending, the PTO initiated a Covered Business Method Review of the '280 Patent, which ContentGuard asserted against Apple, Appx3518, but did not pursue at trial. *See Google Inc. v. ContentGuard Holdings, Inc.*, CBM2015-00040, 2016 WL 3438922 (PTAB June 21, 2016). The PTAB found all challenged claims unpatentable. *Google*, 2016 WL 3438922, *1, *22, *25.[10]

In an effort to salvage some part of its patent, ContentGuard filed a Motion to Amend, *id.* at *25. As it was required to do, *id* at *29 (citing

[10] The PTAB's analysis is fully consistent with the district court's construction of "usage rights." The PTAB observed that "Stefik discloses permanently attaching usage rights to the digital work," that "[c]opies of the digital work also will have the usage rights attached thereto," and that "any usage rights … always will remain with the digital work." *Google*, 2016 WL 3438922, *15.

37 C.F.R. § 42.300(b)), ContentGuard offered constructions for the terms in its proposed amended claim and proposed that the PTAB adopt the same construction of "usage rights"—including "attached, or treated as attached"—that it now challenges on appeal:

In its Motion to Amend, Patent Owner proposes a construction of two claim terms, both of which are reproduced in the table below.

Claim Term	Claim Construction
"content"	"the digital information (i.e. raw bits) representing a digital work"

Claim Term	Claim Construction
"usage rights"	"indications that are attached, or treated as attached, to [a digital work/digital content/content/a digital document] and that indicate the manner in which the [digital work/digital content/content/ digital document] may be used or distributed as well as any conditions on which use or distribution is premised"

Google, 2016 WL 3438922, *29.

ContentGuard assured the PTAB that this construction was not only correct, but "reflects the broadest reasonable construction based on the entirety of the '280 patent disclosure." Patent Owner's Contingent Motion to Amend Under 37 C.F.R. § 42.121, CBM 2015-00040, Paper No. 16 at 6 (Sept. 11, 2015). ContentGuard also told the PTAB that this construction was "based on the '280 patent specification and the disclosure of the Stefik patents incorporated by reference," *i.e.*, the patents asserted here. *Id.* The PTAB accepted that proposed construction and accepted ContentGuard's amended claim. *Id.* at *34.

Having convinced the PTAB to accept the "attached, or treated as attached" construction, ContentGuard cannot now discard that construction to attempt to support its infringement claim. *See Computer Docking Station Corp. v. Dell, Inc.*, 519 F.3d 1366, 1375 (Fed. Cir. 2008) ("Claims should not be construed one way in order to obtain their allowance and in a different way against accused infringers.") (quotation marks omitted); *Microsoft Corp. v. Multi-Tech Sys., Inc.*, 357 F.3d 1340, 1348-50 (Fed. Cir. 2004) (limiting the term "transmitting" to the patentee's construction during prosecution).

Prosecution disclaimer applies to arguments made in reexamination proceedings. *See, e.g.*, *Spectrum Intern., Inc. v. Sterilite Corp.*, 164 F.3d 1372, 1379 (Fed. Cir. 1998) (relying on the patentee's limitation of the claims in reexamination to find noninfringement); *Cole v. Kimberly-Clark Corp.*, 102 F.3d 524, 531-32 (Fed. Cir. 1996) (patentee was "bound" by representations in reexamination and "surrendered" arguments for a broader claim construction). Prosecution disclaimer also applies to positions taken by a patentee concerning a common term in the prosecution or reexamination of a related patent. *See, e.g.*, *Microsoft*, 357 F.3d at 1349 (statement during the prosecution of one

patent relevant to understanding the scope of a common term in two related patents); *Jonsson v. Stanley Works*, 903 F.2d 812, 818 (Fed. Cir. 1990) (prosecution history and construction of a term in one patent relevant to the understanding of the term in a related patent).

Judicial estoppel also bars ContentGuard's inconsistent position in this Court. ContentGuard (1) took a clearly inconsistent position; (2) which if accepted by this Court would create the impression that either it or the PTAB was misled; and (3) such a decision would provide ContentGuard with an unfair advantage. *See New Hampshire v. Maine*, 532 U.S. 742, 750-51 (2001); *see also Rissetto v. Plumbers and Steamfitters Local 343*, 94 F.3d 597, 604 (9th Cir. 1996) (applying judicial estoppel to statements made in an administrative proceeding).

III. THIS COURT SHOULD AFFIRM THE JUDGMENT OF NONINFRINGEMENT.

ContentGuard does not dispute that the jury properly found that Apple does not infringe under the district court's claim construction. Because that claim construction was correct, the judgment should be affirmed. But even under ContentGuard's proposed construction, it failed to prove infringement. The evidence at trial established that Apple's products do not meet other, unchallenged limitations of the

claims. Therefore, the judgment should be affirmed regardless of ContentGuard's "usage rights" argument.

ContentGuard's contention (Br. 37-47) that any modification of the construction of "usage rights" would require a new trial is wrong. First, the legal principle ContentGuard invokes is incorrect. Second, ContentGuard's assertion that the construction of "usage rights" affected "all of Apple's non-infringement arguments" is wrong. Third, ContentGuard misunderstands the burden of proof that applied to its own post-trial JMOL motion and thus mischaracterizes Apple's opposition to that motion.

A. Modification of a Claim Construction Does Not Require a New Trial Where Other Claim Limitations Are Not Met.

Even if it could show that the "attached, or treated as attached" construction of "usage rights" was wrong, ContentGuard would not be entitled to a new trial because Apple's products do not meet limitations of the claims that are unchallenged on appeal. *See SSL Servs.*, 769 F.3d at 1084-85 (rejecting position that party was "entitled to a new trial if [the court] agree[d] that *any one* of the disputed claim constructions was erroneous" because "there is no evidence in the record from which a

good faith argument can be made" that the products at issue met a different limitation). *See also Nuance Commc'ns, Inc. v. ABBYY USA Software House, Inc.*, 813 F.3d 1368, 1374 (Fed. Cir. 2016) ("even if the district court did err in adopting a dictionary definition for the disputed terms, Nuance is not entitled to a new trial because it is clear that 'correction of the errors in [the] jury instruction on claim construction would not have changed the result, given the evidence presented'").

B. Apple's Accused Systems Do Not Meet Unchallenged Portions of the Construction of "Usage Rights."

ContentGuard challenges only the "attached, or treated as attached" portion of the construction of "usage rights." The remainder of that construction was proposed by ContentGuard. Appx25. To establish infringement under that construction, ContentGuard needed to identify "usage rights" which "indicate the manner in which the [digital content] may be used or distributed as well as any conditions on which use or distribution is premised." Appx35. ContentGuard failed to do so.

The evidence established that Apple's accused systems do not include "usage rights," attached or otherwise, that meet the

unchallenged portion of the construction—and no reasonable juror could conclude otherwise. *See Teleflex*, 299 F.3d at 1328 ("We may affirm the jury's findings on infringement or validity issues if substantial evidence appears in the record supporting the jury's verdict and if correction of the errors in a jury instruction on claim construction would not have changed the result, given the evidence presented.").

The evidence demonstrated that Apple controls user access to digital content through account and rental keys. Appx1955-1959(117:4-121:11); Appx2211-2212(77:19-78:7); Appx2900-2904. ContentGuard did not contend that these keys were usage rights. *See supra* at p. 21 n.6. Instead, ContentGuard's expert Dr. Goodrich identified two data elements as alleged "usage rights"—the "kind" and "isRental" fields contained in a "Purchase Response" transmitted within Apple's iTunes system. Appx1105-1107(146:6-148:10).

But the jury heard unrebutted testimony from Apple's engineer that these fields are used only to control how lists of files in the iTunes library are *displayed*. Appx1961(123:9-12) (the "isRental" and "kind" fields are "used to organize and properly present the movie in the library for the user"); Appx2944-2947; Appx2957-2962. No evidence

showed that FairPlay uses any "indications" from those fields to permit or prohibit playback, copying, or other manners of use, as the claim construction requires. Appx1940(102:20-22); Appx1960-1961(122:23-123:8). *See also* Appx1178(41:22-24); Appx2177(43:2-25); Appx2867.

In fact, the jury heard unrebutted testimony to the contrary. As ContentGuard's expert explained, "[i]nformation in the usage rights tells the repository what it can and cannot do with the digital content." Appx1178(41:22-24). An Apple engineer testified without contradiction based on tests he had performed that even if the "isRental" and "kind" fields are removed, the content will still play. Appx1941-1942(103:12-104:10); Appx1944-1945(106:18-107:5); Appx1962-1963(124:6-125:11); Appx2046-2047(57:16-58:25). These tests conclusively proved these fields cannot be "usage rights," regardless of the "attached, or treated as attached" requirement, because they do not "tell[] the repository what it can and cannot do." These fields do not "indicate the manner in which the [digital content] may be used or distributed as well as any conditions on which use or distribution is premised." Appx35. They only tell the iTunes software how to *display* the information about a user's iTunes library, for example, by grouping rented content apart

from non-rented content. Appx2904. No reasonable jury could find that these fields meet ContentGuard's own construction of "usage rights."

C. Apple's Accused Systems Do Not Meet the "Repository" Limitations.

1. The Devices that Make Up Apple's System Do Not Maintain the Required Integrities.

ContentGuard also was required to prove that every device in Apple's accused system that plays a role in the transfer or use of digital content was a repository that maintained the three required integrities in the support of usage rights. Appx2169(35:5-22); Appx2203-2205(69:17-71-17). ContentGuard failed to do so.

Apple's Servers Lack "Behavioral Integrity." Apple's FairPlay servers do not have behavioral integrity at any time, much less in the support of usage rights, because they allow software that does not include a digital certificate to be installed. *See* Appx1952-53(114:18-115:17); Appx2054(65:2-12) Appx2077-79(88:12-90:7); Appx2951-54; Appx2190(56:3-5); Appx2194(60:5-14). ContentGuard's expert admitted there was no evidence that Apple's software updates to FairPlay servers included digital certificates. Appx1467(32:18-22). Apple's witnesses confirmed that there were no digital certificates.

Appx1950-1951(112:13-114:8); Appx2077-2082(88:6-93:19); Appx2190-2193(56:6-59:2).

Apple's Servers Lack "Communications Integrity." Apple's servers do not maintain communications integrity because they communicate with non-repositories in the support of usage rights, including Macs, PCs, AppleTV devices, and Akamai servers. *See* Appx2197(63:7-21); Appx1727(87:1-12); Appx1920(82:4-7); Appx2839-2840.

The jury heard unrebutted testimony that iTunes content can be copied to or from Macs and PCs over insecure connections; software can be installed on Macs and PCs without digital certificates; and iTunes content files can be directly accessed and altered on a Mac or PC. Appx1758-1759(118:21-119:11); Appx1771-1772(131:3-132:12); Appx1983(6:3-20); Appx1927-1928(89:24-90:10); Appx1949-1950(111:2-112:5); Appx1963(125:17-19); Appx2155-2157(21:17-23:20); Appx2294(28:4-11). ContentGuard's own patents and the inventor admit that general purpose computers (*e.g.*, Macs or PCs) "are not trusted systems and cannot be made trusted without significantly altering their architectures." Appx373(2:4-20); Appx967-968(8:17-9:11).

Stefik's contemporaries at Xerox, including inventors on ContentGuard's other patents, likewise explained that Macs and PCs were not trusted systems, and could not easily be made so. Appx3922-3923; Appx979-982(20:16-23:15); Appx2158-2161(24:18-27:16); Appx2850-2852.

ContentGuard offered no evidence whatsoever that the AppleTV was a repository. The jury heard testimony that an AppleTV can play digital works, Appx1751(111:24-25), and that users "can watch iTunes movies and television shows on an AppleTV," Appx1727(87:1-3). The jury also was told that ContentGuard had asserted that AppleTV, as a "product[ ] which utilize[s] DRM such as iTunes," might infringe its patents, Appx4528; Appx1530(56:6-22), but had abandoned that position and AppleTV was not "even accused in this case," Appx1733(93:17-18). In other words, not only was there no affirmative proof that AppleTV is a repository, but by the time of trial ContentGuard *knew* that AppleTV was *not* a repository and had abandoned any claim to the contrary.

ContentGuard also conceded that the Akamai servers that store and distribute Apple's digital content to user devices (and communicate

with Apple's servers) are not repositories. *See* Appx1196(59:5-9); Appx2194-2196(60:15-62:12); Appx2881-2886. Communications with Akamai servers plainly are "in the support of usage rights," because the content resides on those servers (after they acquire it from Apple servers), and they transfer that content to user devices. ContentGuard's expert agreed that transferring content is an action in support of usage rights. Appx3440(88:3-7). And the PTAB recently accepted ContentGuard's argument that communications integrity is required when a client device downloads content from a server. Appx3491-3492. ContentGuard cannot now disavow an argument it made to maintain the patentability of its claims. *See Computer Docking Station Corp.*, 519 F.3d at 1375.

Apple's User Devices Lack Behavioral Integrity. All of Apple's user devices allow the user to install movies, eBooks, and songs without digital certificates. *See* Appx2954-55(116:13-117:1); Appx1468(33:7-12) (ContentGuard's expert admitting he "did not identify digital certificates for installing things like movies, books, music, that sort of thing"); Appx2955; Appx2888-2889. The patents explicitly equate content with software, so behavioral integrity requires

that a digital certificate be included in digital content. *See* Appx195(12:13-14, 12:47-50) (citing "entertainment 'software' such as video and audio recordings by magnetic recorders."); Appx2200-2201(66:17-67:8). And the requirement is not merely a technicality, but directly implicates the security issues the patents supposedly addressed: Apple's expert testified that Apple user devices have been compromised by untrusted code that entered the devices embedded in content files, a result that would not have occurred if the content had included digital certificates. Appx2263(129:19-25); Appx2264(130:11-19); Appx2201(67:9-25). *See also* Appx2044(55:6-12) (book or movie containing executable code would be installed despite lacking a digital certificate). ContentGuard's expert agreed that book or movie files could contain viruses, and conceded that ContentGuard's patents characterize content as software. Appx2507-2509(71:23-73:13).

Apple's User Devices Lack Physical Integrity. Unrebutted testimony established that the devices in the accused iTunes/FairPlay system lack physical integrity, because they permit access to digital content by untrusted systems. Appx23. In particular, Apple's devices provide users direct access to digital content, such that it can be

transferred or altered. *See* Appx2196-2200(62:17-66:11); Appx2291(25:12-24); Appx2293-2294(27:23-28:11) (encryption cannot satisfy physical integrity).

* * *

Any *one* of the defects described above is fatal. No reasonable jury could have concluded that the devices and servers that play an integral role in the delivery and use of content in Apple's system are repositories. Not only does each device fail to satisfy at least behavioral or physical integrity, but each device communicates "in the support of usage rights" with servers (including Akamai and Apple servers) that do not and cannot "present proof that they are trusted systems." Appx20-21. These servers (which are not repositories) communicate "in the support of usage rights" with all of the user devices in the accused Apple system (iPhones, iPads, iPods, Macs, and PCs running iTunes), so none of those devices is a repository either. *See* Appx2292-2293(26:22-27:20) ("[I]f one of these is not a repository, then the communications integrity with that fails, and as a result, you don't have communications integrity in the system."). *See also* Appx2205(71:10-17); Appx373(2:4-6).

2. The Construction of Usage Rights Has No Bearing on ContentGuard's Failure of Proof Regarding the Repository Limitations.

ContentGuard's argument that the supposedly incorrect construction of "usage rights" implicates the "repository" limitations is meritless. (Br. 38.) While it is true that repositories must maintain the required integrities only "in the support of usage rights," that means that regardless of the scope of "usage rights" or "in the support of usage rights," each device in the claimed system must maintain the three integrities at least *some* of the time. As explained above, the evidence established that the computers and devices in Apple's system *never* maintain all three integrities. For example, ContentGuard presented no evidence that Apple's servers, Macs, or PCs ever maintain behavioral integrity or that AppleTV maintains any integrities at any time. Devices that *never* maintain one or more of the three integrities necessarily fail to do so in the support of usage rights.

Second, ContentGuard never explains why removing the "attached, or treated as attached" requirement from the construction of usage rights would have made it easier to prove that Apple's devices are repositories. That has it backwards. What ContentGuard fails to

acknowledge is that a broader construction of "usage rights"—that is, its proposed construction under which usage rights can, but need not, be attached or treated as attached to content—would heighten, not lower, the burden of showing that a particular device qualifies as a "repository," because a repository is defined by its ability to maintain the three integrities in the support of usage rights. That means that the broader the scope of usage rights, the more circumstances under which a device must maintain the three integrities in order to qualify as a repository.

ContentGuard was unable to show that Apple's devices maintained the three integrities even in the narrower situation where "usage rights" must be attached to content, so it could not possibly show that the integrities are maintained where "usage rights" are present in a broader set of circumstances.

D. Apple's JMOL Opposition Is Irrelevant.

ContentGuard's burden in its JMOL motion was to show that *no reasonable jury* could have found for Apple. In opposition to that motion Apple accordingly explained that, on the record here, the jury "could reasonably conclude" that Apple did not infringe and that

ContentGuard therefore was not entitled to JMOL of infringement. ContentGuard collects three pages of such quotations from Apple's opposition (Br. 44-47), then arrives at the surprising conclusion that Apple thereby conceded that a reasonable jury could find *for ContentGuard*. To the contrary, Apple moved for JMOL of noninfringement at the close of the evidence. Appx3697-3717. Apple argued it was entitled to JMOL because ContentGuard failed to establish the repository limitations. *See* Appx3700-3707. Apple also argued that no reasonable jury could find the accused "kind" and "isRental" fields to be "usage rights." Appx3707-3708.

Apple thus maintained that no reasonable jury could have found infringement. Apple's statement that *ContentGuard's* JMOL motion should be denied because a reasonable jury could find for Apple did not change that position or concede that a reasonable jury could also find for ContentGuard.

IV. CONTENTGUARD IS NOT ENTITLED TO A NEW TRIAL BASED ON THE DISTRICT COURT'S EVIDENTIARY RULINGS.

A. ContentGuard Fails Even To Argue That Any Particular Ruling Was An Abuse of Discretion That Affected Its Substantial Rights.

ContentGuard devotes half its brief to arguments concerning alleged deficiencies in Apple's discovery disclosures, but fails to identify any specific rulings to be overturned on appeal—much less explain how they reflect an abuse of discretion. That failure is fatal to ContentGuard's appeal.

ContentGuard's failure has a simple explanation: ContentGuard brought these discovery disputes (complaints about Apple's source code production and the "rsync" issue) to the district court's attention, and in each instance *ContentGuard obtained the relief it requested*. A district court's failure to grant additional, unrequested relief is reviewed for plain error, not abuse of discretion. *United States v. Potts*, 644 F.3d 233, 236 (5th Cir. 2011) ("Plain error review was appropriate, because the defendant effectively received all of the relief that he requested from the district court."). This is because "logically there is little difference between a case that comes to us where no objection has been made to the alleged impropriety and one where no further objection has been

made to the trial judge's handling of an impropriety." *United States v. Carter*, 953 F.2d 1449, 1466 (5th Cir. 1992). ContentGuard does not even suggest that plain error occurred here.

B. ContentGuard's Source Code Complaints Fail Because The Court Granted the Relief ContentGuard Sought and Other Evidence Unequivocally Established Macs and PCs are Not Repositories.

ContentGuard's complaints about Apple's source code production[11] are without merit and waived. ContentGuard argued below that Apple's source code production concerning Macs and PCs had been inadequate and untimely, and asked the court to exclude specific paragraphs of the report of Apple's technical expert, Dr. Kelly. Appx575. The court granted that motion, providing exactly the relief ContentGuard sought. Appx578-579.

Dr. Kelly's trial testimony fully complied with that order, and ContentGuard does not argue otherwise. However, in the middle of trial ContentGuard asked for much broader relief than it had sought in

[11] Although irrelevant to any issue raised by ContentGuard, Apple fully complied with its discovery obligations, and produced more than 180 million lines of source code in this case. Appx4769. ContentGuard's suggestions that Apple refused to produce source code it had been ordered to produce are false.

its *Daubert* motion and that the court had considered appropriate. The court properly ruled that ContentGuard had already received *exactly* the relief it had requested. Appx1145(8:11-16); Appx1943-1944(105:25-106:5). That ruling was not an abuse of discretion, and ContentGuard does not even suggest that it was. A trial court does not abuse its discretion by granting a party the precise relief it seeks in a pretrial motion, and by denying that same party's untimely request for additional relief mid-trial.

Moreover, ContentGuard's argument concerning the source code's relevance to the noninfringement verdict (Br. 50-51) is incorrect. The fact testimony at trial establishing that Macs and PCs are not repositories has *nothing to do with iTunes source code*. As explained above, Apple's witnesses testified concerning the ordinary operation of Macs and PCs, and general aspects of their operating systems, which demonstrated that these computers do not have the integrities required to meet the "repository" limitations, just as ContentGuard's own patents recognized. iTunes content can be copied to or from Macs and PCs over insecure connections; software can be installed on Macs and

PCs without digital certificates; and iTunes content files can be directly accessed and altered on a Mac or PC. *See* Section III.C.1, *supra*.

ContentGuard did not below, and does not on appeal, ever suggest that its review of iTunes source code would have enabled it to refute that testimony. The evidence that Macs and PCs do not meet the "repository" integrity limitations is publicly-available information, readily ascertainable from using or reading about a Mac or PC. It is not based on source code. The alleged source code production deficiencies, even had they occurred, could not have affected ContentGuard's substantial rights.

C. ContentGuard's "rsync" Complaints Rest on a Legally Flawed Infringement Theory and Distortions of the Record.

As explained above, Apple complied with its discovery obligations and its witness gave completely truthful deposition testimony that ContentGuard misrepresents in its brief. After rsync arose again at trial, ContentGuard sought and the court granted ContentGuard the opportunity to present previously-undisclosed expert testimony that Apple's use of rsync supposedly established infringement. Appx2326(60:7-9); Appx2483-2486(47:11-50:9).

Beyond the fact that ContentGuard received the relief it requested, the rsync issue is irrelevant because ContentGuard's new theory of "behavioral integrity" was legally wrong. Moreover, the district court did not abuse its discretion (at least not to ContentGuard's detriment) by permitting ContentGuard to present previously-undisclosed expert testimony advancing that legally-invalid theory.

1. ContentGuard Cannot Prove Behavioral Integrity Based on Secure Communication Protocols.

ContentGuard's failure of proof on behavioral integrity had nothing to do with rsync or any communication channel used to copy software updates to a server. The claims require that the *software* "include a digital certificate"; that is, if a device permits software without a digital certificate to be installed, that device lacks behavioral integrity and is not a repository. Appx21-23. ContentGuard's expert admitted there was no evidence that Apple's software updates included digital certificates. Appx1467(32:18-22). Apple's witnesses confirmed there were no digital certificates. Appx1950-1951(112:13-114:8); Appx2077-2082(88:6-93:19); Appx2190-2193(56:6-59:2). The evidence conclusively demonstrated that Apple's FairPlay servers allowed

software that did not include a digital certificate to be installed, and therefore no reasonable jury could have found infringement.

Recognizing this at trial, ContentGuard stitched together its rsync theory, but it was too little, too late. During discovery, ContentGuard never asked any Apple witness what mechanism Apple used to transfer software updates to its servers, undoubtedly because that mechanism—whatever it was—could not possibly establish behavioral integrity. However software is transferred, if it can be installed on a device without including a digital certificate, that device is not a repository. The software updates installed on the FairPlay servers do not include digital certificates. Appx1467(32:18-22); Appx2191-2192(57:25-58:23); Appx1952-1953(114:18-115:17); Appx2054(65:2-12) Appx2077-2079(88:12-90:7); Appx2951-2954; Appx2190(56:3-5); Appx2194(60:5-14); Appx2875-2878.

ContentGuard does not challenge that undisputed fact. Instead, ContentGuard points to the undisputed but irrelevant fact that the rsync protocol, which is used to move software updates, "relies on a digital certificate exchange." (Br. 10; *see also* Br. 41.) That theory

improperly conflates communications and behavioral integrity.[12] Under the claim construction, behavioral integrity requires that software to be installed in a repository *include* a digital certificate, while the separate requirement of communications integrity demands that *communications* between devices be secure. Appx20-23. ContentGuard's theory that a secure communications connection alone can satisfy both requirements, Appx1190(53:3-6); Appx1191(54:6-16); Appx1194(57:8-16), would vitiate the requirement of behavioral integrity by deeming it satisfied whenever there is communications integrity, Appx1190(53:16-25).

Indeed, there is a critical difference between using a digital certificate to secure a communications channel and including a digital certificate in software to ensure that the software being installed is authentic and has not been altered. Apple engineer Alan Ward explained that a secure connection (even if established using digital certificates) will not stop a computer virus or other unauthorized software that does not include a digital certificate from being installed on a computer. *See* Appx2081(92:1-23); Appx2968. In other words,

[12] ContentGuard concedes that "an exchange of digital certificates" is involved in communications integrity. (Br. 12-13, 41-42.)

even if a digital certificate is used to establish a secure communications channel, that digital certificate cannot ensure that the software file sent over that secure channel is authentic and was not tampered with before it was sent. If the receiving computer does not require that installed software include a digital certificate, that computer has no ability to verify who produced the software or what it might contain. Consistent with that, ContentGuard's expert admitted the secure communication protocol he identified "is not what is commonly referred to as a digital certificate by modern computer scientists." Appx2484-85(48:17-49:9).

Finally, even if a communications protocol (including rsync) could show behavioral integrity, the claim construction demands that the would-be repository *require* that the digital certificate be present for software to be installed. Appx23. ContentGuard offered no evidence that Apple *requires* that the communications protocol used to transfer software to FairPlay servers must be established using digital certificates. In fact, undisputed testimony established that Apple's system does *not* require the use of rsync (or any other secure communication protocol) to install software on FairPlay servers. Appx2087-2089(98:17-100:8); Appx2445(9:12-10:17).

2. ContentGuard's "rsync" Complaints are Meritless.

Rather than concede that Apple does not infringe, ContentGuard coupled its improper legal theory (that a secure communications channel could provide "behavioral integrity") with unjustifiable, after-the-fact accusations that Apple failed to provide ContentGuard with information about rsync that ContentGuard never requested.

As explained above, ContentGuard never asked Apple deponents to identify the utilities Apple uses to copy software updates to the servers. Appx3565-3566; Appx3574-3599; Appx3608(32:2-21); Appx3615(59:13-15; 60:2-7; 61:16-21); Appx3617(67:3-23; 69:1-24); Appx3623(92:24-93:13). Nonetheless, ContentGuard had ample notice that Apple uses rsync in connection with FairPlay file transfer processes, because eight months before trial an Apple engineer identified "rsync" as a utility Apple uses to transfer iTunes content files to the Akamai servers. Appx3673(139:18-19).

ContentGuard's claim that Apple provided "highly misleading or, at worst, false" deposition testimony on software updates—*i.e.*, that a senior Apple engineer and 30(b)(6) representative perjured himself (Br. 23)—is, to borrow ContentGuard's own hyperbolic expression,

"astonishing[]" (Br. 24, 48).[13] Apple's witness testified at deposition that while FairPlay servers had used a single shared file system in the past, there are now approximately 250 servers and each gets its own "local" copy of the software. Appx3615-3617(59:13-61:21). He testified that Apple system administrators manage this update process. *Id*. ContentGuard *never asked* what utility Apple personnel use to copy files to the servers until trial, when Apple's engineer accurately identified rsync.

ContentGuard's efforts to connect rsync to Apple's source code production (Br. 22) are equally unfounded. As explained above, rsync is an open source utility. ContentGuard had notice that Apple uses it in the accused system, yet never asked for any information or raised any issue about rsync with Apple or the district court.

The reason is clear: rsync is irrelevant. rsync is a file transfer tool that copies files from one location to another. ContentGuard's theory evidently is that, if it had had access to rsync code (which, again, it never requested and which is publicly available), ContentGuard

[13] ContentGuard's other characterizations of the rsync issue—that Apple "failed to timely disclose" rsync, "failed to produce the source code," and presented "an unconscionable failure-of-proof argument" at trial (Br. 1-2, 9-10) are equally astonishing, not to mention false.

would have been able to show that this file transfer utility somehow tampers with the contents of files being transferred, by inserting and including within them the digital certificates required to show "behavioral integrity." (*See* Br. 24.) This is nonsense.

Using a digital certificate to open a connection, then using that connection to copy a software file, is not "requiring software to include a digital certificate in order to be installed in the repository," which is what the claim construction requires. Appx23. Thus, regardless of when or how ContentGuard learned about rsync, ContentGuard's arguments provide no basis for a new trial. Moreover, ContentGuard's expert was allowed to offer previously-undisclosed testimony at trial concerning ContentGuard's unfounded, irrelevant theory, and ContentGuard seized that opportunity without complaint. *See* Appx2424(158:19-21); Appx2440-2441(4:8-5:8). ContentGuard therefore suffered no prejudice, much less "substantial harm." *See* 11 Wright, Miller & Kane, *Federal Practice and Procedure* § 2805 (2016).[14]

[14] ContentGuard complains that the court's *in limine* ruling barring the parties from parading discovery disputes before the jury "put ContentGuard in an untenable position" because ContentGuard could not "reveal[] to the jury" that "Apple had deliberately withheld" evidence. (Br. 10.) But, (1) Apple never deliberately withheld anything,

— APPLE'S APPEAL —

V. THE ASSERTED CLAIMS ARE UNPATENTABLE UNDER § 101 AND INVALID UNDER § 103.

If this Court finds that it lacks jurisdiction over ContentGuard's appeal, or affirms the noninfringement judgment on the merits, Apple will voluntarily dismiss its appeal. If, however, this Court concludes that ContentGuard's appeal is properly before it and has merit, then the eligibility and validity issues should be addressed.

A. ContentGuard's Patents Are Drawn to Unpatentable Subject Matter.

Libraries have enforced restrictions and conditions on patrons' use of written works for hundreds of years. Patrons present a library card to borrow a book, and agree to abide by return date or other restrictions. Appx3387-3390. Libraries have expanded this loan system to audio and video recordings. Video rental stores adopted the same concept in the 1980s; video game rental stores did so in the 1990s.

ContentGuard's patents do nothing more than apply the abstract idea of the library loan to digital works, using well-known computing techniques. Claims that "recite only generic computer components

---

and the district court never found that it did; and (2) rsync source code could not possibly have established that any Apple software update "include[d]" a digital certificate.

configured to perform otherwise conventional steps" cannot transform an abstract idea (like enforcing use limitations on works) into patentable subject matter. *Alice Corp. Pty. v. CLS Bank Int'l*, 134 S. Ct. 2347, 2359 (2014).

1. The Asserted Stefik Claims Are Not Patent Eligible.

Claim 6 of the '007 Patent is illustrative, and is drawn to the abstract idea of distributing content subject to usage rights and restrictions. Appx347(50:31-49). That idea—loaning out a book with a due date—is a "fundamental economic practice long prevalent in our system of commerce." *Alice*, 134 S. Ct. at 2356. There is no inventive element that renders this idea patentable. Generic references to "processors" and "instructions" stored in "memories" are insufficient, and "send[ing]" and "determin[ing]" from data are among the "most basic functions of a computer." *Alice,* 134 S. Ct. at 2358-59.

The district court found the claims non-abstract because they require repositories maintaining physical, communications, and behavioral integrity. Appx3555-3556. But these were pre-existing computing concepts that Stefik conceded he did not invent. Appx993-996. "Simply appending conventional steps, specified at a high level of

generality, which are well known in the art and consist of well-understood, routine, conventional activit[ies] previously engaged in by workers in the field, is not sufficient to supply the inventive concept." *Intellectual Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1313 (Fed. Cir. 2016) (quotation marks omitted).

Like Claim 6 of the '007 Patent, Claim 7 of the '956 Patent, claim 1 of the '072 Patent, and claim 1 of the '859 Patent are all drawn to the same abstract idea of restricting access to materials. Appx305(51:43-62); Appx263(52:8-23); Appx215(51:16-38). These claims likewise lack any inventive elements sufficient to make them patentable.

2. Claim 1 of the '053 Patent Fails to Recite Patent-Eligible Subject Matter.

Claim 1 of the '053 Patent builds on the Stefik patents by adding the notion of *creating* usage rights. That abstract legal concept—sublicensing—is not patentable. *Cf. In re Comiskey*, 554 F.3d 967, 981 (Fed. Cir. 2009) (claims "describ[ing] an allegedly novel way of requiring and conducting arbitration…are unpatentable").

The '053 Patent discusses the concepts of "meta-rights" and "state variables," but neither adds anything inventive. A "meta-right" is the right to create, modify, or dispose of usage rights associated with

content, or to create, modify, or dispose of meta-rights themselves. Appx375(5:19-31). That is sublicensing. A "state variable" records the status of a usage right or meta-right. Appx375(5:42-59). For example, a usage right might be the right to make three copies of the content, and a corresponding state variable would record that the patron has made two of the three copies. Bookkeeping does not make sublicensing any less abstract.

During the pre-*Alice* prosecution of the '053 Patent, the examiner rejected the pending claims under Section 101. Appx3326-3330. The inventors amended the claims to provide that the steps were performed "using a processor." Appx3333-3341. Claim 1 would not have issued but for limitations that the Supreme Court has since made clear are insufficient.

B. The Prior Art Presented at Trial Established That The Stefik Patent Claims Are Obvious.

Two prior art academic papers, called ABYSS and Dyad, Appx4017-4030; Appx4031-4062, show that ContentGuard's asserted claims would have been obvious. ContentGuard inventors recognized both ABYSS and Dyad as prior art examples of the "trusted system" approach to DRM. Appx3922; Appx3940. Expert testimony from Dr.

Steve White (the author of the ABYSS reference), along with documentary evidence, provide a clear and convincing showing that the elements of the Stefik patents were well-known before the purported inventions, and that the asserted claims are nothing more than obvious combinations of these well-known elements.

1. The Combination of ABYSS and Dyad Discloses Both Repositories and Usage Rights.

The ABYSS paper describes "A Trusted Architecture for Software Protection." Appx4017. ABYSS discloses a trusted system for DRM involving a "secure coprocessor" that ensures content is used only subject to "rights-to-execute." Appx2342-2343(76:25-77:10); Appx2344(78:2-13). The "rights-to-execute" indicate how the content can be used, and the secure coprocessor checks those rights to ensure they are satisfied before the content is accessed. Appx2344(78:14-24). Dyad discloses "A System for Using Physically Secure Coprocessors" that expressly "builds on" the ABYSS trusted system by adding digital certificates. Appx4031; Appx2337(71:2-25); Appx2345(79:6-14); Appx2345-2346(79:15-80:16). It was undisputed that one of skill in the art would have been motivated to combine these references—they are in effect already combined by the Dyad paper. Appx2518(82:9-15).

Dyad and ABYSS together teach a skilled person to use repositories having the three "integrities." DRM systems taught by Dyad and ABYSS are tamper-proof (they maintain physical integrity), transfer data over secure communication channels (they maintain communications integrity), and require digital certificates to install software (they maintain behavioral integrity). Appx2345(79:6-14); Appx2358(92:13-22); Appx2360(94:5-11); Appx2362(96:8-18); Appx2364-65(98:3-99:7); Appx4018, Appx4028-4029 (physical security and secure channels between secure processors in ABYSS); Appx4036, Appx4041-4042, Appx4048, Appx4050 (physical security, secure coprocessors, and digital certificates in Dyad).

The combination of Dyad and ABYSS also discloses DRM systems that have usage rights—a "right to execute"—that are attached or treated as attached to content, and which include manners of use. Appx2366(100:3-13); Appx2367-2368(101:19-102:8); Appx2352(86:6-20); Appx4018-4019, Appx4023, Appx4029 (describing right-to-execute in ABYSS). Dr. White testified that in November 1994 there was nothing "new and inventive about usage rights attached or treated as attached to content being used on a Stefik-type repository." Appx2356(90:13-25).

Each of the other elements of the asserted claims pursued at trial is also present in the combination of Dyad and ABYSS. *See* Appx2368-2370(102:19-104:20) ('859 claim 1); Appx2370-2372(104:21-106:1) ('072 claim 1); Appx2372(106:2-23) ('956 claim 7); Appx2372-2373(106:24-107:13) ('007 claim 6).

2. ContentGuard Failed To Rebut The Substantial Evidence of Invalidity.

ContentGuard advanced only two challenges to Dr. White's testimony. First, ContentGuard's expert claimed that Dyad and ABYSS do not teach behavioral integrity. *See* Appx2491-2492(55:2-56:3). But he addressed only whether each reference *individually* does so. *See In re Keller*, 642 F.2d 413, 426 (C.C.P.A. 1981) ("[O]ne cannot show non-obviousness by attacking references individually where, as here, the rejections are based on combinations of references"). He failed to address whether the *combination* of Dyad and ABYSS made behavioral integrity obvious, and Dr. White established that they did.

ContentGuard's expert also failed to address other evidence showing that behavioral integrity was obvious, including a Xerox white paper describing Dyad and ABYSS as trusted systems, the ABYSS and Dyad articles themselves, and documents explaining that using digital

certificates to check software before installing it had been well known since at least 1980. Appx2362-2364(96:19-98:2); Appx2373-2374(107:14-108:2); Appx4048; Appx4050; Appx4089; Appx3922. *See also* Appx2513-2514(77:7-78:8); Appx3968.

Dr. Goodrich also testified concerning supposed secondary considerations, *see* Appx2493-2495(57:10-59:23), but he did not and could not testify that any secondary considerations had any nexus to the asserted claims. *See Geo. M. Martin Co. v. All. Mach. Sys. Int'l LLC*, 618 F.3d 1294, 1305 (Fed. Cir. 2010); *Ormco Corp. v. Align Tech., Inc.*, 463 F.3d 1299, 1311-12 (Fed. Cir. 2006). The evidence showed there was no nexus. *See* Appx2119(130:9-10); Appx4748; Appx2521(85:19-20); Appx956-957(124:25-125:1); Appx963(4:3-11).

C. The Asserted Claims Of The '053 Meta-Rights Patent Are Invalid As Obvious Based On The Stefik '980 Patent.

U.S. Patent No. 5,629,980 ("Stefik '980"), a related Stefik patent that ContentGuard did not assert at trial, makes obvious every element of the processes and systems claimed in claim 1 of the '053 Patent.

1. The '053 Patent Acknowledges Stefik '980 As Prior Art and Adds No Non-Obvious Additional Limitations.

The '053 Patent incorporates the Stefik '980 patent by reference, Appx373-374(1:50-56, 2:22-24, 2:66-3:22), and purports to build on it by including "meta-rights" and "state variables." But "meta-rights" (the right to create or modify usage rights) and "state variables" (representing the status of a usage right) necessarily already exist in any Stefik system. If content in a Stefik system has "usage rights," something must have created them—that is, a "meta-right" necessarily existed. If "it may be desirable to limit the number of copies of a digital work," such that "[w]hen the Copy-Count equals zero, the [Copy] right can no longer be exercised," Appx199(20:13-24), some variable tracking the status of copy counts must already be present.

The differences between Stefik '980 and the '053 Patent are differences of nomenclature, not substance. For example, the "Next-Set-of-Rights" in Stefik '980 specifies the usage rights that a recipient of the "Next-Set-of-Rights" may grant to another entity. Appx3996-3997(20:55-21:14). The "Next-Set-of-Rights" is a "right that, when exercised, creates or disposes of usage rights (or other meta-rights) but

that is not itself a usage right because exercising a meta-right does not result in action to content"—*i.e.*, a meta-right. Appx108. Stefik '980 also describes state variables to track the status of rights. Appx3991-3992(10:24-11:14 & Table 1) (describing "information relating to the state of a right" and different property-value pairs for state variables). The '053 Patent purports to add state variables *identifying a location* and *sharing* rights to the incorporated-by-reference Stefik DRM scheme, but these ostensible differences are actually described in Stefik '980 or, at a minimum, are obvious and insignificant modifications. *See infra,* pp. 89-90.

2. The Stefik '980 Patent Discloses Or Makes Obvious Every Limitation Of Claim 1 Of The '053 Patent.

Stefik '980 specifically discloses or makes obvious each of the steps of the "method for sharing rights adapted to be associated with an item" of claim 1 of the '053 Patent.

"specifying…at least one usage right and at least one meta-right…"

This limitation requires that the system include a usage right or meta-right that can be shared—for example, a right to view a movie on a user's computer as well as on her phone. Likewise, the '053 Patent

acknowledges that systems for interpreting and enforcing "meta-rights" were known in the prior art. Appx373(1:50-56, 2:37-41); Appx374(4:65-67); Appx375(6:23-25) ("meta-rights" are operationally the same as usage rights, and "[t]he interpretation and enforcement of usage rights are well known generally"). Stefik '980 discloses meta-rights themselves, and describes a framework that enables their implementation using repositories. *See, e.g.*, Appx3992(11:36-44).

In particular, Stefik '980's "Next-Set-of-Rights" "defines how rights are carried forward for a copy of a digital work." Appx3996(20:55-58). Stefik '980 discloses three kinds of rights, called Copy, Transfer, and Loan, which can include a "Next-Copy-Right" designation that "determine the rights on the work after it is transported." Appx3992(19:62-64, FIG. 15, element 1505); *see also* Appx4003-4004(34:36-36:27). These designations of next (*i.e.*, downstream) rights act to create or dispose of usage rights. They are "meta-rights" as the district court construed that term in the '053 Patent because they are not themselves usage rights, but are used to create usage rights. *See* Appx108 (a meta-right is "a right that, when exercised, creates or disposes of usage rights (or other meta-rights) but

that is not itself a usage right because exercising a meta-right does not result in action to content.").

Stefik '980 explains that state variables (*e.g.*, "copy count") are included in the rights. Appx3995(18:23-41). It also discloses sharing of rights by disclosing sharing of state variables. For example, Stefik '980 explains that "[t]he number of copies that could be loaned is the sum of the Copy-Counts for all of the versions of the loan right of the digital work." Appx4002(32:1-3). When this right is exercised, "[t]he server updates the usage rights information in the digital work to reflect the number of copies loaned out." Appx4004(35:57-58). Stefik '980 further explains that "copy count" (a state variable associated with each right, Appx3997(21:18-20)) is shared among one or more users or devices by being decremented each time a right is exercised by any user or any device, Appx3997(21:20-21). Stefik '980 thus discloses that copy rights are shared among one or more users or devices.

"defining…a manner of use…"

Stefik '980 shows that a set of rights can be obtained by the requestor when the creator of a work attaches usage rights "to a digital work, and store[s] them in [a repository]." Appx3990(7:6-37);

Appx3974. This set of rights can be "usage rights," and it "corresponds to a particular way in which a digital work may be used or distributed." Appx3995(18:23-41); Appx3990(7:6-37). The label of the transactional component of the "usage right" defines the manner of permitted use "*e.g.*, COPY or PRINT." Appx3995(18:23-28). In the Glossary section, Stefik '980 further explains that its "usage rights" define "the manner in which a digital work may be used or distributed, as well as any conditions on which use or distribution is premised." Appx4012(51:64-67). These "usage rights" are defined by repositories, which include processors. Appx3988(4:6-9); Appx3993(14:13-20).

"defining…a manner of rights creation for the item"

Stefik '980 discloses a framework that allows creation of usage rights by transferring rights from one device/user to another. Appx3992(11:36-44). As discussed above, the "Next-Set-of-Rights" provides a meta-right that defines a manner of rights creation for the item. *Id.*

"said at least one meta-right is enforceable by a repository and allows said one or more users or devices to create new rights"

In Stefik '980, all rights, including meta-rights, are enforced by repositories. Appx4002(31:26-30); Appx3989(6:57-61) ("The

enforcement elements of the present invention are embodied in repositories. Among other things, repositories are used to … maintain the security and integrity of the system."). These are the same repositories used in the Stefik patents. Appx373:1:50-56; Appx101. Stefik '980's scheme also provides for the creation of rights based on the meta-rights that can allow usage rights to be modified as they are passed down to another user/device. In particular, rights can be added, deleted, or replaced by the repositories as the works are received, using the "Add," "Delete," and "Replace" grammar elements. Appx3996(20:55-58, 20:60-65); Appx3982(FIG. 15, element 1509).

"associating…one state variable with the at least one right…"

Stefik '980 discloses examples of "state variables," including "Copy Count," "Loan-Period," "Remaining-Time," and "History-list," which track the states of the created rights. Appx3997(21:15-24); Appx3991-3992(10:46-11:14). According to ContentGuard, an identifier can be a state variable that identifies a location. *See* Appx1232(95:15-23). When state variables are stored in a memory location, they necessarily identify a location where that state of rights is tracked. In addition, Stefik '980 discloses a "state variable" called "Revenue-Owner" that is

"a handle identifying a revenue owner for a digital work. This is used for reporting usage fees." Appx3991-3992(10:66-11:7). The identifier is used when connecting to a credit server to track whether a user has paid the appropriate fees to exercise a right. Appx3995(17:6-13).

Alternatively, there can be no genuine dispute that identifying a location where a state variable is tracked would have been obvious to a computer scientist. Identifying locations of variables is a conventional computer programming technique. *See* Appx1241(104:1-22).

"generating…one or more rights based on the meta-right in the first license, wherein the one or more rights in the second license includes at least one right that is shared among one or more users or devices"

Stefik '980 explains that when a request for a loan or copy of a digital work is made by the requesting repository, the sending repository will transfer a copy of the work with rights specified by the "Next-Set-Of-Rights." Appx3996(20:55-67); Appx4004(35:15-21). The "Next-Set-Of-Rights" is the meta-right in the first license, and the rights specified by the "Next-Set-Of-Rights" are generated rights of the second license. As explained above, Stefik '980 discloses sharing of usage rights.

"associating at least one state variable with the at least one right that is shared in the second license"

In Stefik '980, as discussed above, rights are shared among one or more users or devices by limiting the number of copies that can be created by copying, transferring, or loaning. In Stefik '980, the "usage right" in the second license can also include "copy counts," which (as discussed above) are state variables related to the number of copies that can be made, and are associated with that usage right. Appx3995(18:23-41).

"wherein the at least one state variable that is associated with the second license is based on the at least one state variable that is associated with the first license"

As explained above, the rights generated in the second license (and the state variables within the rights of the second license) are shared with the rights in the first license (and the state variables within the rights of the first license). For example, Stefik '980 shows how a digital work can be played, transferred, deleted, or loaned by the following right: "((Play) (Transfer) (Delete)(Loan 2 (Delete: Transfer Loan))." Appx3999(25:59-65). Here, the meta-right in the first license (*i.e.*, Loan Right) can create a usage right (*e.g.*, Play Right) in the second license. The usage right in the second license references the Copy-

Count and Copies-in-Use state variables that are based on information in the "Next-Set-Of-Rights" meta-right of the first license. Appx3991(10:51-53, 35:14-21, 35:58-59). In particular, the Copies-in-Use state variable is incremented when a Loan transaction is completed and the Copy-Count state variable is decremented. Appx3997(21:20-21); Appx4002(31:59-62, 32:24-26); Appx4004(35:24-25, 36:8-13).

D. Apple Is Entitled in the Alternative to a New Trial on Invalidity.

At a minimum, Apple is entitled to a new trial on invalidity under Rule 59(a). In light of ContentGuard's failure to rebut the clear and convincing evidence of obviousness of the four Stefik patents, and with the plain disclosures of the alleged inventive elements of the '053 Patent found in a single prior art reference, the determination that the asserted patents are not invalid was against the great weight of the evidence, justifying a new trial. Moreover, Apple's invalidity arguments were presented based on a construction of "usage rights" that ContentGuard seeks to broaden on appeal. If this Court were to modify that construction as ContentGuard urges, Apple would be entitled to demonstrate on remand the invalidity of those broader claims. *See*

Cardiac Pacemakers, Inc. v. St. Jude Med., Inc., 576 F.3d 1348, 1356 (Fed. Cir. 2009) (en banc).

VI. CONCLUSION

The noninfringement judgment should be affirmed. The district court properly construed the "usage rights" limitation of all the asserted claims, and ContentGuard admittedly failed to prove infringement under that construction. Moreover, the overbroad construction of "usage rights" ContentGuard urges on appeal would not change the result, because there was no evidence that Apple's accused products met other, unchallenged limitations of the claims. If the Court were to reach the issues presented by Apple's appeal, the Court should hold the asserted claims invalid under Section 101 or Section 103. Alternatively, Apple is entitled to a new trial on invalidity.

Respectfully submitted,

Dated: November 14, 2016

/s/ Constantine L. Trela, Jr.
Constantine L. Trela, Jr.
David T. Pritikin
Nathaniel C. Love
SIDLEY AUSTIN LLP
One South Dearborn Street
Chicago, IL 60603
(312) 853-7000

Jeffrey P. Kushan
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
(202) 736-8000

Counsel for Apple Inc.

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a)(7)(B). The brief contains 16,482 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(iii) and Fed. Cir. R. 32(b).

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). The brief has been prepared in a proportionally spaced typeface using Microsoft Word 2007 in 14-point Century Schoolbook font.

Dated: November 14, 2016

/s/ Constantine L. Trela, Jr.
Constantine L. Trela, Jr.
SIDLEY AUSTIN LLP
One South Dearborn Street
Chicago, IL 60603
(312) 853-7000

Counsel for Apple Inc.

CERTIFICATE OF SERVICE

I hereby certify that on this 14th day of November, 2016, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Federal Circuit using the Court's CM/ECF system, which will send notifications to all counsel registered to receive electronic notices.

/s/ Constantine L. Trela, Jr.
Constantine L. Trela, Jr.
Counsel for Apple Inc.