Nos. 2019-2192, -2258

United States Court of Appeals for the Federal Circuit

TECSEC, INC.,

Plaintiff-Appellant,

v.

ADOBE INC.,

Defendant-Cross-Appellant,

SAS INSTITUTE, INC., SAP AMERICA, INC., SAP AG, CISCO SYSTEMS, INC., SYBASE, INC., SOFTWARE AG, SOFTWARE AG, INC., ORACLE CORPORATION, ORACLE AMERICA, INC.,

Defendants.

Appeals from the United States District Court for the Eastern District of Virginia in No. 1:10-cv-00115-LO-TCB, Judge Liam O'Grady.

REPLY BRIEF OF CROSS-APPELLANT

Tara D. Elliott
Michael A. Morin
Gabriel K. Bell
Rachel Weiner Cohen
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004
(202) 637-2200
tara.elliott@lw.com

Counsel for Cross-Appellant Adobe Inc.

February 3, 2020

CERTIFICATE OF INTEREST

Counsel for Appellee certifies the following:

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

   Adobe Inc.

2. The name of the real party in interest (if the party named in the caption is not the real party in interest) represented by me is:

   Not applicable.

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

   None.

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

   Latham & Watkins LLP: Maximilian A. Grant, Dale Chang, Brett M. Sandford, Gabrielle LaHatte.

   Christian & Barton, LLP: Michael W. Smith, Roman Lifson, David B. Lacy.

   Constantine Cannon LLP: Henry C. Su.

   Allen & Overy LLP (asterisk denotes no longer with the firm): Riccardo S. Macchiaroli*, Steven E. Adkins*.

   Greenberg Traurig LLP (asterisk denotes no longer with the firm): Vivian S. Kuo, William P. Nelson*, Christina M. Finn*, James F. Valentine*.

   Dewey & LeBoeuf LLP (asterisk denotes no longer with the firm): Lyle Roberts*, Andrew N. Stein*, Christina M. Finn*, Henry C. Bunsow*.

   Law Office of Craig C. Reilly: Craig C. Reilly.

Fenwick & West LLP (asterisk denotes no longer with the firm): Charlene M. Morrow, David Wallace*, Phillip J. Haack*, Virginia K. DeMarchi*, Rebecca A.E. Fewkes, Jeffrey A. Ware, Dargaye H. Churnet, Yixin Zhang*, Kunyu Ching*, Bryan A. Kohm, Amy E. Hayden*, Christopher L. Larson.

Howrey LLP (asterisk denotes no longer with the firm): Henry C. Bunsow*.

John Steele, Attorney at Law: John J. Steele.

5. The title and number of any case known to counsel to be pending in this or any other court or agency that will directly affect or be directly affected by this court's decision in the pending appeal. *See* Fed. Cir. R. 47.4(a)(5) and 47.5(b).

   The district court proceedings that were not subject to the Rule 54(b) judgment currently on appeal could be affected by this appeal. *See TecSec, Inc. v. SAS Institute, Inc., SAP America, Inc., SAP AG, Cisco Systems, Inc., Sybase, Inc., Software AG, Software AG, Inc., Adobe Inc., Oracle Corp., Oracle America, Inc.*, Case No. 1:10-cv-00115-LO/TCB.

Dated: February 3, 2020

Respectfully submitted,

/s/ Tara D. Elliott
Tara D. Elliott

TABLE OF CONTENTS

Page

CERTIFICATE OF INTEREST i

TABLE OF AUTHORITIES iv

INTRODUCTION 1

ARGUMENT 2

I. TECSEC DOES NOT DISPUTE THAT CLAIMS 1 AND 8 OF THE '702 PATENT ARE REPRESENTATIVE OF ALL ASSERTED CLAIMS 2

II. THE ASSERTED CLAIMS ARE INELIGIBLE UNDER § 101 2

A. The Claims Are Directed To An Abstract Idea 2

1. Reciting "Multi-Level Security" Does Not Make The Claims Non-Abstract 3

2. The Other Features TecSec Cites Do Not Make The Claims Non-Abstract 8

3. TecSec's Reliance On Adobe's Prior Statements Is Misleading And Unavailing 12

4. The Cases TecSec Relies On Are Inapposite 13

B. The Claims Add Nothing Inventive To The Abstract Idea 15

CONCLUSION 19

TABLE OF AUTHORITIES

Page(s)

CASES

Alice Corp. Pty. Ltd. v. CLS Bank International,
573 U.S. 208 (2014).....11, 15, 19

Amdocs (Israel) Ltd. v. Openet Telecom, Inc.,
841 F.3d 1288 (Fed. Cir. 2016) 17, 18

Ancora Technologies, Inc. v. HTC America, Inc.,
908 F.3d 1343 (Fed. Cir. 2018) 13

Athena Diagnostics, Inc. v. Mayo Collaborative Services, LLC,
915 F.3d 743 (Fed. Cir. 2019) 17

BASCOM Global Internet Services, Inc. v. AT&T Mobility LLC,
827 F.3d 1341 (Fed. Cir. 2016) 17, 18

Bridge & Post, Inc. v. Verizon Communications, Inc.,
778 F. App'x 882 (Fed. Cir. 2019) 7, 9

BSG Tech LLC v. Buyseasons, Inc.,
899 F.3d 1281 (Fed. Cir. 2018) 16

Chamberlain Group, Inc. v. Techtronic Industries Co.,
935 F.3d 1341 (Fed. Cir. 2019) 15, 16

Content Extraction & Transmission LLC v. Wells Fargo Bank, National Association,
776 F.3d 1343 (Fed. Cir. 2014) 5

CyberSource Corp. v. Retail Decisions, Inc.,
654 F.3d 1366 (Fed. Cir. 2011) 7

DDR Holdings, LLC v. Hotels.com, L.P.,
773 F.3d 1245 (Fed. Cir. 2014) 6, 14, 15

Enfish, LLC v. Microsoft Corp.,
822 F.3d 1327 (Fed. Cir. 2016) 14, 15

Page(s)

FairWarning IP, LLC v. Iatric Systems, Inc.,
839 F.3d 1089 (Fed. Cir. 2016) 7

Intellectual Ventures I LLC v. Capital One Bank (USA),
792 F.3d 1363 (Fed. Cir. 2015) 5, 13

Intellectual Ventures I LLC v. Capital One Financial Corp.,
850 F.3d 1332 (Fed. Cir. 2017) 6

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

Internet Patents Corp. v. Active Network, Inc.,
790 F.3d 1343 (Fed. Cir. 2015) 6

Mortgage Grader, Inc. v. First Choice Loan Services Inc.,
811 F.3d 1314 (Fed. Cir. 2016) 2, 12

Parker v. Flook,
437 U.S. 584 (1978).....8

Prism Technologies LLC v. T-Mobile USA, Inc.,
696 F. App'x 1014 (Fed. Cir. 2017) 7, 9

RecogniCorp, LLC v. Nintendo Co.,
855 F.3d 1322 (Fed. Cir. 2017) ..... *passim*

SAP America, Inc. v. InvestPic, LLC,
898 F.3d 1161 (Fed. Cir. 2018) 3, 7, 16

Smart Systems Innovations, LLC v. Chicago Transit Authority,
873 F.3d 1364 (Fed. Cir. 2017) 9

SRI International, Inc. v. Cisco Systems, Inc.,
930 F.3d 1295 (Fed. Cir. 2019) 13, 14

TecSec, Inc. v. Adobe Systems Inc.,
658 F. App'x 570 (Fed. Cir. 2016) 3, 10, 13

TecSec, Inc. v. International Business Machines Corp.,
731 F.3d 1336 (Fed. Cir. 2013) 10, 11

Page(s)

In re TLI Communications LLC Patent Litigation,
823 F.3d 607 (Fed. Cir. 2016) 10

Two-Way Media Ltd. v. Comcast Cable Communications, LLC,
874 F.3d 1329 (Fed. Cir. 2017) 4, 11

Versata Development Group v. SAP America, Inc.,
793 F.3d 1306 (Fed. Cir. 2015) 6

STATUTES

35 U.S.C. § 101 1

INTRODUCTION

The asserted claims are invalid for lack of eligible subject matter under 35 U.S.C. § 101 because they (1) focus on an abstract concept (managing access to objects using multiple layers of encryption and labels) and (2) add nothing inventive. Red Br. 59-72. TecSec's brief does not undermine that conclusion. Yellow Br. 39-60. TecSec does not, and cannot, identify anything that makes its claims non-abstract at *Alice* step one or inventive at *Alice* step two. The asserted claims provide no specific improvement in the functioning of computer or network technology and, instead, require only conventional components recited at a high level of generality, which is insufficient to confer eligibility. Notably, TecSec's own technical expert conceded that the claims require no improved encryption algorithms, computer components, or network technology: "the specific encryption algorithm *is not important—any algorithm* can be used," Appx1967 ¶ 38, and "[t]he data network and components of a computer or computer network *were known*," Appx1964 ¶ 29 (emphases added). Therefore, if this Court reaches Adobe's cross-appeal, it should find the asserted claims ineligible under § 101.[1]

[1] Adobe raises the claims' lack of patent-eligible subject matter conditionally in this cross-appeal. The Court need not reach that issue unless it otherwise declines to affirm the district court's judgment in full.

ARGUMENT

I. TECSEC DOES NOT DISPUTE THAT CLAIMS 1 AND 8 OF THE '702 PATENT ARE REPRESENTATIVE OF ALL ASSERTED CLAIMS

TecSec does not dispute that claims 1 and 8 of the '702 patent (Appx239-240) are representative for purposes of § 101. Red Br. 61; *see* Appx1886 ("TecSec agrees that claims 1 and 8 are representative of the asserted method and system claims, respectively, for purposes of an analysis under 35 U.S.C. § 101."); Appx4 ("The parties agree that claims 1 and 8 in the '702 Patent are representative . . . ."). Consequently, all asserted claims rise or fall with claims 1 and 8. *See RecogniCorp, LLC v. Nintendo Co.*, 855 F.3d 1322, 1324 n.1 (Fed. Cir. 2017) (patentee waives argument by not asserting that "each asserted claim must be analyzed separately"); *Mortg. Grader, Inc. v. First Choice Loan Servs. Inc.*, 811 F.3d 1314, 1324 n.6 (Fed. Cir. 2016) ("no need to address . . . claims individually" as there is "no contention that the claims differ in any manner that is material to . . . patent-eligibility").

II. THE ASSERTED CLAIMS ARE INELIGIBLE UNDER § 101

A. The Claims Are Directed To An Abstract Idea

Under *Alice* step one, the asserted claims are directed to the abstract concept of managing access to objects using multiple layers of encryption and labels. Red Br. 61-68. TecSec's brief does not show otherwise.

1. Reciting "Multi-Level Security" Does Not Make The Claims Non-Abstract

TecSec principally relies on the claims' recitation of "'multi-level' security," *i.e.*, "nesting" one encrypted object within another. Yellow Br. 44-57. However, nesting (embedding data within other data) is the heart of the abstract idea itself, which cannot make the claims eligible. Red Br. 6, 63-64, 67-68, 72; *see*, *e.g.*, *SAP Am., Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1163 (Fed. Cir. 2018) (purported advance in computerized claims cannot be abstract idea).[2] TecSec's arguments to the contrary fail for four reasons.

First, the claims recite no specific way of improving computer technology to perform multi-level security. *See RecogniCorp*, 855 F.3d at 1326 (claims directed to abstract idea absent "'specific means or method' for improving technology"). The representative claims include a single, vague reference to "multi-level security" in the preamble with no detail, let alone any technological improvement, in how to embed data within other data. Appx239-240 (cls. 1, 8). Indeed, this Court held that the claimed "multi-level security" can be as simple as embedding one encrypted object (such as a PDF) within another. *TecSec, Inc. v. Adobe Sys. Inc.* ("*TecSec II*"), 658 F. App'x 570, 584 (Fed. Cir. 2016) (software "performs [the claimed] multi-

[2] TecSec's assertion that Adobe did not "address[] the 'nesting' aspect of 'multi-level security'" (Yellow Br. 53-54) is baseless. Adobe addressed it repeatedly. Red Br. 6, 63-64, 67-68, 72.

level security when a user encrypts a PDF, then attaches it to a separate PDF, and then encrypts that PDF"). And the specification admits that such embedding can be performed with "standard" off-the-shelf software, "such as Microsoft's Object Package for Windows." Appx236 (5:34-37, 5:49-51). Reciting the "abstract end-result" of multi-level security "'using conventional computer activity,'" without how to perform it, does not make the claims non-abstract. *RecogniCorp*, 855 F.3d at 1326 (ineligible claims for encoding and decoding data); *see also Two-Way Media Ltd. v. Comcast Cable Commc'ns, LLC*, 874 F.3d 1329, 1333, 1337 (Fed. Cir. 2017) (ineligible claim for controlling and routing data packets to multiple recipients "d[id] not sufficiently describe how to achieve these results in a non-abstract way"); Red Br. 67-68 & n.20.[3]

Second, the concept of multi-level security is akin to human activities, not a uniquely computer-based solution to a computer-specific problem. *Id.* at 63-64. In TecSec's own telling, multi-level security provides "the ability to nest or embed encrypted objects in other encrypted objects" such that multiple recipients "hav[e] separate access permissions." Yellow Br. 47. But that same concept is reflected, for example, in "nesting" multiple locked offices (each accessible to a single person)

[3] The "means for embedding" term that TecSec quotes (Yellow Br. 45) is irrelevant because it appears only in claim 9, not in representative claims 1 and 8. Appx239-240. Regardless, it is an aspect of the abstract idea, *supra* at 3, and the specification admits that embedding requires only "standard" software, Appx236 (5:34-37).

within a locked office building (accessible to multiple people) or "nesting" multiple lockboxes within a secure bank vault. Indeed, the patent itself analogizes the purported invention to a series of nested containers secured by traditional metal keys, Appx228 (Fig. 3), and analogizes the encrypted "objects" to things "in your daily life" that "may contain other objects," such as "[y]our car" or "desks," Appx235 (3:33-37). *See* Red Br. 63-64. Such brick-and-mortar analogues further confirm that the claims are directed to an abstract idea at step one. *See, e.g.*, *Intellectual Ventures I LLC v. Capital One Bank (USA)* ("*Capital One I*"), 792 F.3d 1363, 1369-70 (Fed. Cir. 2015) (claims for tailoring online content, akin to regional newspapers or television advertisements, were abstract at *Alice* step one).

It does not matter that the security problem might be more acute with respect to electronic data, which can be transmitted "instantaneous[ly] and limitless[ly]." Yellow Br. 49. That is true of any claims addressing alleged problems relating to electronic data. For example, in *Intellectual Ventures I LLC v. Symantec Corp.* ("*Symantec*"), the claims purportedly improved email systems to filter unwanted content such as spam—a growing problem in electronic communications. 838 F.3d 1307, 1314-18 (Fed. Cir. 2016). Nonetheless, this Court held that the claims were akin to humans screening and filtering paper mail and recited no improved computer technology. *Id.*; *see also RecogniCorp.*, 855 F.3d at 1326 (claims for encoding and decoding computer data were akin to Morse Code); *Content Extraction &*

Transmission LLC v. Wells Fargo Bank, Nat'l Ass'n, 776 F.3d 1343, 1347 (Fed. Cir. 2014) (claims for recognizing computer data were akin to activities "humans have always performed" even though "human minds are unable to process and recognize the stream of bits" as in the claimed automated process). Likewise, here, the claims address familiar human and business concerns and the purported benefits stem not from a specific advance in computer technology but from using the abstract "multi-level security" idea in a "'particular technological environment'"—which does not make it "'any less abstract.'" *Symantec*, 838 F.3d at 1314, 1316 (citations omitted).[4]

Third, this Court has found that claims for nesting data (even encrypted data) inside other data provided no patent-eligible advance in technology. For example, in *Intellectual Ventures I LLC v. Capital One Fin. Corp.*, the ineligible claims used "nested [data] structures" to purportedly improve compatibility of documents in a "specialized . . . computer language" ("XML"). 850 F.3d 1332, 1338-39 (Fed. Cir. 2017). In *Versata Development Group v. SAP America, Inc.*, the ineligible claims recited a purportedly improved "hierarchical data structure." 793 F.3d 1306, 1327

[4] Even if multi-level security had no human analogue, the claims' high-level recitation of that concept would not make the claims non-abstract. *Supra* at 3-4; *see Symantec*, 838 F.3d at 1319 (claims directed to abstract idea of "computer virus screening" even though it "originated in the computer era"); *Internet Patents Corp. v. Active Network, Inc.*, 790 F.3d 1343, 1348 (Fed. Cir. 2015) (claims directed to abstract idea of "retaining information in the navigation of online forms"); *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1258 (Fed. Cir. 2014) ("[N]ot all claims purporting to address Internet-centric challenges are eligible for patent.").

(Fed. Cir. 2015). And, in *Bridge & Post, Inc. v. Verizon Communications, Inc.*, the ineligible claims recited "encrypting" a "request identifier," "embedding" it in an "HTTP extensible field," transmitting the "tagged" data, and "decod[ing]" it. 778 F. App'x 882, 888-89 (Fed. Cir. 2019). This Court also found ineligible claims that purportedly enhanced electronic data security by, for example, controlling access to computer resources, *Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App'x 1014, 1016-17 (Fed. Cir. 2017), identifying improper access to computer data, *FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d 1089, 1093 (Fed. Cir. 2016), and identifying fraudulent online credit card transactions, *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1373-74 (Fed. Cir. 2011). *See also* Red Br. 67 n.19. As in those cases, the claims' high-level recitation of multi-level security is equally abstract and ineligible here.

Fourth, TecSec's assertion that multi-level security was "novel" (Yellow Br. 51) and "not found in the prior art" (*id*. at 45) also misses the mark. Even if that abstract concept was new—indeed, "brilliant" or "groundbreaking"—it would not make the claims eligible because a "*new* abstract idea is still an abstract idea." *SAP*, 898 F.3d at 1163 (citations omitted). That is, even if "the claims may not have been anticipated or obvious because the prior art [computer systems] did not disclose [multi-level security], that does not suggest that the idea . . . is not abstract." *Symantec*, 838 F.3d at 1315; *see id*. at 1318 ("[I]nquiry is not whether conventional

[devices] already apply" the abstract concepts.); *Parker v. Flook*, 437 U.S. 584, 588 (1978) (claims ineligible even assuming they were "novel and useful").

2. The Other Features TecSec Cites Do Not Make The Claims Non-Abstract

The litany of other "steps and components" that TecSec lists (Yellow Br. 44-45) also does not make the asserted claims non-abstract.

First, the encryption "modules" and labelling "subsystem[s]" (*id*.) are merely functionally-named components for performing encryption and labelling, which are aspects of the abstract idea. Red Br. 65-66 & n.17. The claims do not purport to improve—or provide any details for implementing—the encryption and labelling functions. To the contrary, the specification admits that existing systems (which were "incorporated by reference [t]herein") limited access based on labeling and encryption (Appx234 (2:31-61)), as TecSec acknowledges (Yellow Br. 54 n.16). Moreover, TecSec's technical expert, Dr. Jones, expressly admitted that the claims provide no improved encryption algorithm: "the specific encryption algorithm *is not important—any algorithm* can be used." Appx1967 ¶ 38 (emphasis added); *see also* Appx12756-12758 (521:21-523:17) (Jones) (admitting that "'encryption algorithm

module' . . . is going to basically provide encryption algorithms" and that labelling "'subsystem'" is "responsible for creating the label"); Red Br. 66 n.17.[5]

As discussed, this Court has found abstract (and ineligible) claims for encoding or encrypting data, *see RecogniCorp*, 855 F.3d at 1326; *Bridge & Post*, 778 F. App'x at 888-89, and claims for securing access based on labels or other identifying information, *see Smart Sys. Innovations, LLC v. Chicago Transit Auth.*, 873 F.3d 1364, 1369 (Fed. Cir. 2017) (ineligible claims for "validating entry" into a transit system using "a bankcard verification system"); *Prism*, 696 F. App'x at 1016 (ineligible claims for an "authentication server" to receive identity data and permit access based on authenticity). *See* Red Br. 66-67 & n.19; *supra* at 5-7. Reciting functional components for performing such conventional activities does not make the claims non-abstract. *See, e.g.*, *Symantec*, 838 F.3d at 1316-19 (ineligible claims

[5] TecSec does not, and cannot, meaningfully dispute that "using encryption and labels are commonplace computer tasks." Yellow Br. 54 n.16. In addition to the specification itself (Appx234 (2:31-61)), the Pond and Preston references cited on the face of the '702 patent (Appx225) leave no doubt that that encryption and labeling were well known. *See* Appx469 (Pond) (5:16-17) ("data ciphering . . . is well known in the art"); Appx497 (Preston) (1:14-23) (describing art from 1989 that taught "a *labeling* mechanism which enabled *encryption* of a file and also enabled a limited number of access restrictions to the file[,] . . . such as the file owner, the company, and the machine" (emphasis added) (citing Appx463-471 (Pond))). The prosecution history confirms the same. After the '702 patent claims were rejected as anticipated, the applicant admitted that prior art "discloses a multiple user stored data *cryptographic labeling* system that uses labels to control access to data files" and overcame the rejection only by amending the claims to recite embedding objects. Appx531 (emphasis added); *see* Appx441-446; Appx518-533; Appx536-538.

had subcomponents such as "receipt mechanism" for receiving data and "rule engine" for applying rules to filter data); *In re TLI Commc'ns LLC Patent Litig.*, 823 F.3d 607, 614-15 (Fed. Cir. 2016) (ineligible claims had subcomponents such as "image analysis unit" and "control unit"); Red Br. 65-66.

Second, the "object-oriented key manager" ("OOKeyMan") (Yellow Br. 44) is merely the "software component that manages the encryption of an object," *TecSec II*, 658 F. App'x at 582—another necessary aspect of the abstract idea. As construed by this Court, it requires no improved computer technology and instead only needs to perform "one or more" of the conventional functions that any encryption key manager would perform—*i.e.*, "generating, distributing, changing, replacing, storing, checking on, and destroying cryptographic keys." *Id.* The fact that the claims recite encrypting an "object" is immaterial: the "object" can be "any distinct, separate entity" (Appx27009), including any "information" or "data files." Appx235 (3:42-57); *see TecSec, Inc. v. Int'l Bus. Machs. Corp.* ("*TecSec I*"), 731 F.3d 1336, 1346 (Fed. Cir. 2013). That strikingly broad definition confirms that the key manager requires no improved computer technology.

Third, the other three claimed features that TecSec identifies—a "digital logic means," "system memory means," and "data network" (Yellow Br. 44)—also require no improved computer technology. This Court held that the "digital logic means" includes any computer circuitry and the "system memory means" includes

any memory component (*e.g.*, "RAM"). *TecSec I*, 731 F.3d at 1347-48; Red Br. 66. And the patent and TecSec's expert admit that the claims can use any known "data network." Appx236 (5:42-43) ("encrypted object(s) can be easily transported/routed over *any* network" (emphasis added)); Appx1964 ¶ 29 ("The data network and components of a computer or computer network were known . . . .").

It is settled law that performing claims using such generic memory or processing devices or "in a network" does not make them eligible. *See, e.g.*, *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 226 (2014) (claims ineligible despite "data processing system" with a "communications controller" and "data storage unit"); *Symantec*, 838 F.3d at 1319-20 (claims ineligible despite performing virus screening concept "in the . . . network"); *Two-Way*, 874 F.3d at 1333, 1337 (claims ineligible despite controlling and sending data packets to multiple recipients "in a network"). At most, those features provide a "particular [computerized] technological environment," which does not make claims non-abstract. *Symantec*, 838 F.3d at 1319.

Fourth, unable to find the requisite technological improvement in the text of the representative claims (claims 1 and 8), TecSec invokes the "various 'means plus function limitations' set forth in claim 12." Yellow Br. 45. But those terms are irrelevant because TecSec conceded that claims 1 and 8 are representative and it is too late for TecSec to back away now. *See RecogniCorp*, 855 F.3d at 1324 n.1;

Mortg. Grader, 811 F.3d at 1324 n.6; *supra* at 2. And, as this Court held in *TecSec I* (and Adobe explained), the terms in claims 1 and 8 were *not* means-plus-function terms; the district court erred in holding otherwise. Red Br. 66, 70-71.[6] In any event, TecSec does not, and cannot, explain why any differences in claim 12 are relevant to the eligibility analysis. Instead, TecSec concedes that claim 12 is "virtually identical" to the representative claims. Yellow Br. 45. And, as discussed, the representative claims (and thus all asserted claims) are directed to an abstract idea.

3. TecSec's Reliance On Adobe's Prior Statements Is Misleading And Unavailing

TecSec quotes several snippets from prior Adobe briefs that, according to TecSec, are "in direct contradiction to what [Adobe] asserts now." *Id*. at 45-46; *see also id*. at 53, 58. That argument is meritless. The cited statements—which describe the claims as requiring multi-level security using encryption and labeling (Appx27317, Appx27331, Appx27333)—are fully consistent with Adobe's description of the claims in this appeal. *See, e.g*., Red Br. 61-62 (summarizing steps of claim 1). Adobe never suggested (let alone "acknowledged," Yellow Br. 44) that any of the claimed features make the claims eligible under § 101. Those statements did not address § 101 *at all*. They are, instead, taken from Adobe's briefing in favor of summary judgment of non-infringement, *see* Appx27326-27339 (arguing accused

[6] TecSec does not contest that the district court simply misinterpreted *TecSec I*. Red Br. 70-71.

products do not meet "multi-level security," "object-oriented key manager," and "label" limitations); Corrected Response Br. of Appellee Adobe Sys. Inc., *TecSec, Inc. v. Adobe Sys. Inc.*, No. 15-1686, 2015 WL 6083511, at *5 (Fed. Cir. Sept. 30, 2015)—which this Court ultimately *rejected* in *TecSec II*, 658 F. App'x at 576-85, 587 (vacating and remanding summary judgment of non-infringement). TecSec "disingenuous[ly]" (Yellow Br. 53) neglects to mention that fact. Indeed, the fact that this Court found TecSec's claims swept more broadly further highlights their ineligibility. *See Capital One I*, 792 F.3d at 1369 (claims' "breadth" confirms abstraction at step one).

4. The Cases TecSec Relies On Are Inapposite

TecSec's claims are nothing like the specific improvements in computer technology this Court found eligible in the handful of cases that TecSec cites at *Alice* step one. Yellow Br. 50 (citing *Ancora Techs., Inc. v. HTC Am., Inc.*, 908 F.3d 1343, 1348-49 (Fed. Cir. 2018); *SRI Int'l, Inc. v. Cisco Sys., Inc.*, 930 F.3d 1295, 1303 (Fed. Cir. 2019)). In *Ancora*, the claims provided a "non-abstract computer-functionality improvement" that "solve[d] a specific computer [hacking] problem" with a "specific technique" using a "verification structure" containing a "license record" that is "stored in a particular, modifiable, non-volatile portion of the computer's BIOS." 908 F.3d at 1345, 1348-49. In *SRI*, the claims recited "an improvement in computer network technology"—a "specific technique" providing

better security using "network monitors that each analyze specific types of data on the network" and "integrating reports from the monitors." 930 F.3d at 1303. By contrast, TecSec's claims provide no specific improved encryption techniques or improvements in network technology. *Supra* at 3-12. As noted, TecSec's expert conceded that "the specific encryption algorithm is not important—any algorithm can be used"—and "[t]he data network and components of a computer or computer network were known." Appx1967 ¶ 38, Appx1964 ¶ 29.

TecSec also cites unremarkable legal propositions from *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327 (Fed. Cir. 2016), and *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245 (Fed. Cir. 2014), without explaining why the claims in those cases are comparable to the asserted claims here. Yellow Br. 43, 47-51, 54. They are not. In *Enfish*, the claims were eligible because they recited a "specific implementation" of improved computer storage technology—an innovative self-referential database structure that, unlike conventional databases, allowed for adding new fields "on-the-fly" without completely rewriting the database structure. 822 F.3d at 1333, 1339. In *DDR Holdings*, the claims were eligible because their specific innovation (a different way of accessing websites) was "necessarily rooted in computer technology" to solve an "Internet-centric problem" (web site customers being instantaneously transported to another site) that "does not arise in the 'brick and mortar' context." 773 F.3d at 1257-59. TecSec's claims, however, "do not

'improve the functioning of the computer itself,' for example by disclosing an 'improved, particularized method of digital data compression,' or by improving 'the way a computer stores and retrieves data in memory.'" *Symantec*, 838 F.3d at 1315 (quoting *Alice*, 573 U.S. at 225; *DDR Holdings*, 773 F.3d at 1259; *Enfish*, 822 F.3d at 1339). TecSec's claims address a problem commonplace in the brick and mortar context. *Supra* at 4-6. And TecSec's patent and expert admit that the claims do not improve encryption algorithms or network technology and require only conventional components. *Supra* at 8-11. At step one, TecSec's claims are directed to the abstract idea of managing access to objects using multiple layers of encryption and labels.

B. The Claims Add Nothing Inventive To The Abstract Idea

The asserted claims add nothing inventive to the abstract idea at step two. Red Br. 68-70. TecSec makes three arguments. Yellow Br. 57-60. All fail.

First, TecSec principally contends that the claims as a whole—including the abstract idea—"provide a new combination of steps in a way that is unconventional." *Id.* at 57; *see id*. at 59 ("inventive concept" is "'multi-level security' along with various encryption and labelling steps"). That is not the test. "The appropriate question [at step two] is *not* whether the entire claim as a whole was 'well-understood, routine [and] conventional'" but rather whether, "'apart from'" the abstract idea, the additional elements add something inventive. *Chamberlain Grp., Inc. v. Techtronic Indus. Co.*, 935 F.3d 1341, 1348-49 (Fed. Cir. 2019) (emphasis

added); *see also BSG Tech LLC v. Buyseasons, Inc*., 899 F.3d 1281, 1290 (Fed. Cir. 2018) ("[R]elevant inquiry is not whether the claimed invention as a whole is unconventional or non-routine."); *SAP*, 898 F.3d at 1163 ("Nor is it enough for subject-matter eligibility that claimed techniques be novel and nonobvious . . . ."); *Symantec*, 838 F.3d at 1318 ("[I]nquiry is not whether conventional computers already apply" abstract idea.). Put differently, TecSec is relying on the abstract idea itself to supply the inventive concept, which is improper. *BSG*, 899 F.3d at 1290 ("claimed invention's use of the ineligible concept to which it is directed cannot supply the inventive concept"); *SAP*, 898 F.3d at 1163 (abstract idea implemented in computer context, even if "[g]roundbreaking" or "brilliant," is not inventive).

Under the proper analysis, the claims add nothing inventive apart from the abstract idea. Red Br. 68-70. Indeed, putting aside the abstract multi-level security idea, the specification discloses that the remaining encryption, labeling, and embedding concepts are wholly conventional, not inventive. Red Br. 6, 62; Appx234 (1:28-2:4, 2:31-61); Appx236 (5:34-37); *see also* Appx7980 (claimed invention "takes existing encryption, label, and object embedding technology, and applies them with predictable results").[7]

---

[7] TecSec's argument that "Adobe has not established that 'multi-level security' or object-level encryption, labelling and nesting is an abstract idea" (Yellow Br. 58) highlights TecSec's error. At step two, it is already established that the claims are directed to an abstract idea and the inquiry is whether anything *else* supplies an inventive concept. *Chamberlain*, 935 F.3d at 1348-49; *BSG*, 899 F.3d at 1290.

Second, the other features TecSec identifies (Yellow Br. 58-59) likewise add nothing inventive. As discussed, the object-oriented key manager (OOKeyMan) is merely a functional component that performs key management, which is a conventional and necessary aspect of encryption. *Supra* at 10. Also, "the various 'means plus function limitations' set forth in claim 12 of the '702 Patent" (Yellow Br. 59) are irrelevant because they are not found in the representative claims and, regardless, provide nothing inventive. *Supra* at 11-12.

Third, TecSec's reliance on Adobe's prior briefs is again inapposite. They are consistent with Adobe's description of the asserted claims here but, in any event, are irrelevant because they come from Adobe's arguments for summary judgment—which this Court ultimately rejected in *TecSec II*. *Supra* at 12-13. The fact that this Court previously reversed the district court's summary judgment of non-infringement confirms that the claims are even broader, and more preemptive, than Adobe argued at that time. *Id.*[8]

The two cases TecSec cites in passing are inapt. Yellow Br. 59-60 (citing *BASCOM Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341 (Fed. Cir. 2016); *Amdocs (Isr.) Ltd. v. Openet Telecom, Inc.*, 841 F.3d 1288 (Fed. Cir.

[8] "Preemption is sufficient to render a claim ineligible under § 101, but it is not necessary." *Athena Diagnostics, Inc. v. Mayo Collaborative Servs., LLC*, 915 F.3d 743, 752 (Fed. Cir. 2019). The district court erred in requiring complete preemption, as Adobe explained, Red Br. 71-72, and TecSec does not contest.

2016)). In *BASCOM*, the eligible claims recited particular improved computer technology—a specific "non-conventional and non-generic arrangement" of network components including a user-customizable network filter at a specific, unconventional location—not just "an abstract-idea-based solution implemented with generic technical components in a conventional way." 827 F.3d at 1350-51. In *Amdocs*, the claims were eligible (based on a narrow claim construction) because they required the components to "operate in an unconventional manner" to provide an "unconventional technological solution (enhancing data in a distributed fashion) to a technological problem (massive record flows which previously required massive databases)." 841 F.3d at 1300-01.

In contrast, here, "[t]here is not . . . any 'specific or limiting recitation . . . of . . . improved computer technology.'" *Symantec*, 838 F.3d at 1316 (citation omitted) (distinguishing such cases). TecSec's asserted patents do not claim any non-conventional arrangement of network components, *BASCOM*, 827 F.3d at 1350, or teach how to operate any particular computer architecture "in an unconventional manner," *Amdocs*, 841 F.3d at 1300-01. Again, the patent and TecSec's expert concede that the claims do not purport to improve either network technology ("any" network will suffice, Appx236 (5:42-44)) or encryption technology ("the specific encryption algorithm is not important—any algorithm can be used," Appx1967 ¶ 38). *Supra* at 8-11. Instead, the asserted claims recite result-oriented functional

limitations to implement the abstract idea of managing access to objects using multiple layers of encryption and labels in a particular technological environment, which is insufficient. Red Br. 68-70; *see Alice*, 573 U.S. at 223 (limiting idea "to a particular technological environment" is insufficient under § 101 (citation omitted)). The asserted claims do not add an inventive concept at *Alice* step two.

CONCLUSION

For the foregoing reasons, and those discussed in Adobe's principal brief, if (and only if) this Court does not otherwise affirm the district court's judgment in full, then the Court should hold that the asserted claims are ineligible under § 101.

Respectfully submitted,

/s/ Tara D. Elliott

Tara D. Elliott
Michael A. Morin
Gabriel K. Bell
Rachel Weiner Cohen
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004
(202) 637-2200
tara.elliott@lw.com

Counsel for
Cross-Appellant Adobe Inc.

February 3, 2020

CERTIFICATE OF SERVICE

I hereby certify that on February 3, 2020, I caused the foregoing Reply Brief of Cross-Appellant to be served by electronic means through the Court's CM/ECF system on counsel for all parties who are registered CM/ECF users.

/s/ Tara D. Elliott
Tara D. Elliott

CERTIFICATE OF COMPLIANCE WITH RULE 32

Pursuant to Fed. Cir. R. 28.1(c) and Fed. R. App. P. 32(g), I hereby certify that this brief complies with the type-volume limitations of Fed. R. App. P. 28.1(e) and Fed. Cir. R. 28.1(b)(3) because it contains 4,469 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f) and Fed. Cir. R. 32(b).

I further certify that this brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) because this brief was prepared using Microsoft Word 2016 in 14-point Times New Roman font.

/s/ Tara D. Elliott
Tara D. Elliott