UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Compass Bank, Commerce Bancshares, Inc., and First National Bank of Omaha
Petitioners

v.

Intellectual Ventures II LLC
Patent Owner

Patent No. 6,314,409
Filing Date: October 26, 1998
Issue Date: November 6, 2001
Title: SYSTEM FOR CONTROLLING ACCESS AND DISTRIBUTION OF DIGITAL PROPERTY

Inter Partes Review No. Unassigned

PETITION FOR *INTER PARTES* REVIEW UNDER 35 U.S.C. §§ 311-319 AND 37 C.F.R. § 42.100 *ET SEQ.*

TABLE OF CONTENTS

LIST OF EXHIBITS

Exhibit 1001: Expert Declaration of Jack D. Grimes, Ph.D. ("Grimes Dec.")

Exhibit 1002: U.S. Patent No. 6,314,409 to Schneck ("'409 patent")

Exhibit 1003: File history of the '409 patent (U.S. Patent Application No. 09/178,606) ("'606 application")

Exhibit 1004: U.S. Patent No. 5,109,413 to Comerford ("Comerford")

Exhibit 1005: U.S. Patent Application No. 06/927,629 ("'629 application")

Exhibit 1006: U.S. Patent No. 4,817,140 to Chandra ("Chandra")

Exhibit 1007: U.S. Patent No. 5,148,481 to Abraham ("Abraham")

Exhibit 1008: U.S. Patent Application No. 06/927,309 ("'309 application")

Through counsel, Compass Bank, Commerce Bancshares, Inc., and First National Bank of Omaha (collectively, "Petitioners") hereby petition for *inter partes* review ("IPR") under 35 U.S.C. §§ 311-319 and 37 C.F.R. § 42 of claims 1-11, 13-21, 23-27, 29-30, 32-33, and 36-39 of U.S. Patent No. 6,314,409 ("'409 patent") and assert that there is a reasonable likelihood that they will prevail with respect to at least one of the claims challenged in this petition.

I. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(a)(1)

A. Real Party-In-Interest under 37 C.F.R. § 42.8(b)(1)

BBVA Compass Bancshares, Inc., Compass Bank, Commerce Bancshares, Inc., Commerce Bank, First National Bank of Omaha, and First National of Nebraska, Inc. are the real parties-in-interest for the instant petition.

B. Related Matters under 37 C.F.R. § 42.8(b)(2)

Intellectual Ventures II LLC ("IV") has asserted the '409 patent in eight pending lawsuits: (1) *Intellectual Ventures II LLC v. BBVA Compass Bancshares, Inc. and Compass Bank d/b/a BBVA Compass*, No. 2:13-cv-01106 (N.D. Ala.); (2) *Intellectual Ventures II LLC v. Commerce Bancshares, Inc. and Commerce Bank*, No. 2:13-cv-04160 (W.D. Mo.); (3) *Intellectual Ventures II LLC v. First National Bank of Omaha*, No. 8:13-cv-00167 (D. Neb.); (4) *Intellectual Ventures II LLC v. JP Morgan Chase & Co., JPMorgan Chase Bank, N.A., and Chase Bank USA, N.A.*, No. 1:13-cv-03777 (S.D.N.Y.); (5) *Intellectual Ventures II LLC v. SunTrust Banks, Inc. and SunTrust Bank*, No. 1:13-cv-02454 (N.D. Ga.); (6) *Intellectual*

Ventures II LLC v. U.S. Bancorp and U.S. Bank, No. 0:13-cv-02071 (D. Minn.); (7) *Intellectual Ventures II LLC v. Huntington Bancshares Inc. and The Huntington National Bank*, No. 2:13-cv-00785 (S.D. Ohio); (8) *Intellectual Ventures I LLC and Intellectual Ventures II LLC v. Capital One Financial Corp., Capital One Bank (USA), N.A., and Capital One, N.A.*, No. 8:14-cv-00111 (D. Md.). IV filed the action against Compass, and served the complaint, on June 12, 2013. IV filed the action against Commerce on June 20, 2013, and served the complaint on June 21, 2013. IV filed the action against First National Bank of Omaha on May 29, 2013, and served the complaint on June 3, 2013. IBM has filed two petitions for IPR of the ’409 patent, *see* IPR2014-00672 and IPR2014-00673, and this is one of two petitions for IPR of the ’409 patent that Petitioners will file on the same day.

C. Lead and Back-Up Counsel and Service Information under 37 C.F.R. § 42.8(b)(3) and (4)

Petitioners provide the following designation of counsel. A power of attorney is being filed with the designation of counsel in accordance with 37 C.F.R. § 42.10(b). Petitioners consent to electronic service by email at the email addresses listed below.

LEAD COUNSEL	BACK-UP COUNSEL
Joseph Melnik (Reg. No. 48,741) (jmelnik@jonesday.com) Jones Day 1755 Embarcadero Road Palo Alto, CA 94303 T: (650) 739-3939; F: (650) 739-3900	Geoffrey K. Gavin (Reg. No. 47,591) (ggavin@jonesday.com) Jones Day 1420 Peachtree Street, N.E., Suite 800 Atlanta, GA 30309-3053 T: (404) 521-3939; F: (404) 581-8330
BACK-UP COUNSEL	BACK-UP COUNSEL
Marc Vander Tuig (Reg. No. 57,964) (mvandertuig@senniger.com) Senniger Powers LLP	Jason S. Jackson (Reg. No. 56,733) (jason.jackson@kutakrock.com) Kutak Rock LLP

100 North Broadway, 17th Floor St. Louis, MO 63102 T: (314) 345-7019; F: (314) 345-7600	1650 Farnam St., The Omaha Building Omaha, Nebraska 68102 T: (402) 231-8359; F: (402) 346-1148

II. PAYMENT OF FEES – 37 C.F.R. § 42.103

This petition for IPR requests review of thirty-three (33) claims. The undersigned authorize the PTAB to charge the fee set forth in 37 C.F.R. § 42.15(a) for this petition to Deposit Account No. 503013, ref: 318208-615002.

III. REQUIREMENTS FOR IPR UNDER 37 C.F.R. § 42.104

A. Grounds For Standing under 37 C.F.R. § 42.104(a)

Petitioners certify that the ’409 patent is eligible for IPR and that they are not barred or otherwise estopped from requesting IPR challenging the identified claims on the grounds identified within the present petition.

B. Identification of Challenge under 37 C.F.R. § 42.104(b) and Relief Requested

Petitioners request IPR in view of the following prior art references:

- U.S. Patent No. 5,109,413 to Comerford (“Comerford”) (Exhibit 1004), which incorporates by reference the disclosure of U.S. Patent Application No. 06/927,629 (“’629 application”) (Exhibit 1005), which issued as U.S. Patent No. 4,817,140 to Chandra (“Chandra”) (Exhibit 1006), issued on April 28, 1992. It is prior art to the ’409 patent under 35 U.S.C. § 102(b).
- U.S. Patent No. 5,148,481 to Abraham (“Abraham”) (Ex. 1007) issued on September 15, 1992. It is prior art to the ’409 patent under 35 U.S.C. § 102(b).

Petitioners submit that claims 1-11, 13-21, 23-27, 29-30, 32-33, and 36-39 of the ’409 patent are invalid based on the following grounds: Ground 1: Comerford anticipates claims 1-11, 13, 21, 23-25, 30, 32-33, 36, and 38 under 35 U.S.C. § 102(b); Ground 2: Comerford in view of Abraham renders claims 14-20, 26-27, 29, 37, and 39 obvious under 35 U.S.C. § 103(a). An explanation of how each claim is unpatentable is set forth below at Section VI. A List of Exhibits is provided with this petition. Included at Exhibit 1001 is the Expert Declaration of Jack D. Grimes, Ph.D. (“Grimes Dec.”) (Exhibit 1001). Pursuant to 35 U.S.C. § 311(b), this petition only includes grounds that could be raised under 35 U.S.C. §§ 102 or 103 on the basis of prior art patents or printed publications.

IV. SUMMARY OF THE ’409 PATENT

A. Brief Description

The ’409 patent is a digital rights management (“DRM”) patent.[1] (Ex. 1001, Grimes Dec., at ¶ 30.) Data owners and distributors were hesitant to expand into the marketplace of networked computers because they were concerned about their lack of control over their digital data after its initial distribution because it could copied and distributed with ease. (*Id.*; *see* Ex. 1002, ’409 patent, 1:14-2:61.) And, the ’409 patent proposed to address this problem by protecting digital data, using encryption as one technique, and then limiting access to the unprotected digital data by enforcing rules defining access rights to the digital data. (Ex. 1001, Grimes Dec., at ¶ 30; *see, e.g.*, Ex. 1002, ’409 patent, Abstract, 6:63-8:2.)

[1] For the state-of-the-art at the time of invention, *see* Ex. 1001, Grimes Dec., at ¶¶ 26-27.

Like the digital data, the rules can be protected, using encryption as one technique, and both the protected digital data and the rules are packaged and distributed to users. (*See* Ex. 1002, ’409 patent, 7:32-41; Ex. 1001, Grimes Dec., at ¶ 31.) The ’409 patent describes transmitting information “openly, that is, using mechanisms and media that are subject to access and copying,” and it lists many means of distribution, “including networks, magnetic media, CD-ROM, semiconductor memory modules, and wireless broadcast and the like.” (*E.g.*, Ex. 1002, ’409 patent, 15:25-28, 32:57-61.)

Fig. 2 of the ’409 patent illustrates the concept of packaged data. (Ex. 1001, Grimes Dec., at ¶ 32.) Data owners and distributors determine what portions of data need to be protected, and this data is included in the encrypted body part 120 of the packaged data, while the data that is not to be protected is included in the unencrypted body part 122 of the packaged data. (*Id.*; *e.g.*, Ex. 1002, ’409 patent, 13:11-18.) Also included in the packaged data are the encrypted rules 124, although they may be provided separately. (Ex. 1001, Grimes Dec., at ¶ 32; Ex. 1002, ’409 patent, 10:47-54.)

Enforcement of the rules is performed by an access mechanism. (Ex. 1001, Grimes Dec., at ¶ 33; *see, e.g.*, Ex. 1002, ’409 patent, 10:1-5.) “The access mechanism 114 allows a user 104 to access the data in packaged data 108 (or 150) according to the rules provided with (or separately from, as packaged rules 152) the packaged data and prevents the user or anyone else from accessing the data other than as allowed by the rules.” (Ex. 1002, ’409 patent, 15:31-35.) Because the access mechanism enforces the rules in this manner, “each and every access to an unprotected form of the protected portions of the data is limited in accordance with rules defining access rights to the data." (*Id.* 35:37-40; Ex. 1001, Grimes Dec., at ¶ 33.) Because the digital data is protected, using encryption as one technique, access to the data that is not "in accordance with [the] rules defining access rights to the data as enforced by [the] access mechanism" (i.e., "unauthorized access") "is not to the unprotected form of the protected portions of the data." (Ex. 1001, Grimes Dec., ¶ 33; Ex. 1002, '409 patent, 35:37-42.) One hardware embodiment disclosed in the '409 patent includes various computer components (e.g., processor, memory, I/O controller, display, encryption hardware), and it discloses protection of the access mechanism using tamper detection. (*See, e.g.*, Ex. 1002, '409 patent, Abstract, 7:6-9, 7:16-22, 7:39-48, 8:38-49, 8:65-67, 15:41-49, 15:65-67, 16:27-30, 27:9-10; Ex. 1001, Grimes Dec., at ¶ 33.)

B. Summary of the Prosecution History of the '409 Patent

The '409 patent's application was filed on October 26, 1998. (Ex. 1003, '606 application, at 1.[2]) It claimed priority to an application filed on January 11, 1996. (*Id.* at 138.) During prosecution, the Examiner questioned how data can be unprotected if access to the data is limited. (*Id.* at 230.) The Examiner also cited U.S. Patent No. 3,648,020 to Tateisi as anticipating and rendering obvious certain claims with reference to its disclosure of a

[2] Here, and elsewhere where a page number is provided instead of column and line numbers, the identified page number refers to the page number provided along with the exhibit number on each page of the exhibit.

number maintained on the magnetic stripe of a bank card. (*Id.* at 231-34.) The applicants explained that "'limited' was meant to refer to controlling access to the data" and that "access to unprotected data might still be controlled, i.e., limited." (*Id.* at 245.) Further, they explained that "[i]n some embodiments, the transformation of data to a protected form is by encryption . . ., although protection is not limited to encryption." (*Id.*) According to the applicants, "the unprotected form of the protected data is generally considered to be the same as the data itself," and "the protected form of the data is generally considered to be different from the data itself." (*Id.* at 246.) Additionally, the applicants argued that in Tateisi "[n]one of the information or data (including the secret number) are stored in any secure or protected manner or form." (*Id.* at 250.) The number (i.e., a PIN) "is called a secret number because it is merely 'known to the owner of the card.'" (*Id.*) Eventually, claims 1-43 issued. (*Id.* at 270; Ex. 1002, '409 patent, 35:32-40:47.)

V. CLAIM CONSTRUCTIONS UNDER 37 C.F.R. § 42.104(b)(3)

Pursuant to 37 C.F.R. § 42.100(b), and solely for the purpose of this review, Petitioners construe the claim language such that the claims are given their broadest reasonable construction in light of the specification of the '409 patent. For terms not specifically listed and construed below, Petitioners construe them for purposes of this review in accordance with their plain and ordinary meaning under the required broadest reasonable construction.

- ***"access mechanism"*** (claims 1, 14, 16, 18-19, 21, 23-26, 30, 32-33, 36-39): "hardware and/or software for controlling access to data." The access mechanism "takes the packaged data . . . and enables the user to access the data in various ways, depending on the access rules." (Ex. 1002, '409 patent, 10:1-5.) It is described throughout the specification. (*Id.* 7:39-49, 8:21-27, 8:52-9:3, 10:1-5, 15:30-21:19, 21:45-57, 31:20-32, 32:29-53, 34:29-43, Figs. 1, 5, 8-16, claims 1, 14, 16, 18-19, 21-26, 30-42.)
- ***"means for storing the rules," "storage means for storing the rules"*** (claims 25, 30, 32-33, 36, and 38): "function: storing the rules"; "structure: volatile and/or non-volatile memory." (*Id.* 8:39-46, 15:41-49, 16:12-22, 19:31-27, 20:17-19, 26:7-10, Fig. 8.)
- ***"means for displaying the images represented by the accessed data"*** (claim 25): "function: displaying the images represented by the accessed data"; "structure: a display monitor." (*Id.* 15:41-59, 17:24-27, 17:37-40, 25:16-22, 26:12-29, 26:54-67, 27:11-13, Figs. 8-9.)
- ***"means for outputting the images represented by the accessed data"*** (claim 30): "function: outputting the images represented by the accessed data"; "structure: a display monitor or printer." The '409 patent describes these as "output devices." (*Id.* 10:34-39, 15:50-54, 17:24-40, 26:12-24, 27:11-24, Figs. 8-9.)
- ***"means for outputting the output signal represented by the accessed data"*** (claim 32): "function: outputting the output signal represented by the accessed data"; "structure: an I/O controller." (*Id.* 15:41-61, 26:12-24, Fig. 8.)

- *“means for generating the output signal from the accessed data”* (claim 33): “function: generating the output signal from the accessed data”; “structure: an I/O controller.” (*Id.* at 15:41-61, 26:12-24, Fig. 8.)

Because the standard for claim construction at the Patent Office is different than that used during a U.S. district court litigation, *see In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1364, 1369 (Fed. Cir. 2004), Petitioners expressly reserve the right to argue a different claim construction in litigation for any term of the ’409 patent as appropriate in such proceeding.

VI. THERE IS A REASONABLE LIKELIHOOD THAT AT LEAST ONE CLAIM OF THE ’409 PATENT IS UNPATENTABLE

As detailed below, the identified references demonstrate that all of the limitations of claims 1-11, 13-21, 23-27, 29-30, 32-33, and 36-39 were known in the prior art at the time of invention. For those claims shown to be rendered obvious in light of a combination of prior art references, the inventions claimed in the ’409 patent are no more than “[t]he combination of familiar elements according to known methods” that “do[] no more than yield predictable results.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 416 (2007). The claims of the ’409 patent are no more than “the predictable use of prior art elements according to their established functions.” *Id.* at 417.

A. Structure of the Claims of the ’409 Patent

Certain claim limitations of the ’409 patent are repeated using substantially similar language. (Ex. 1001, Grimes Dec., at ¶ 35.) These limitations are anticipated or rendered obvious by the same disclosures in the relevant prior art references. To avoid repetition, in the claim charts in Sections VI, full text citations are included the first time the limitations are addressed, but subsequently, only pinpoint citations are provided along with a cross-reference to the full text citations.

B. Comerford Anticipates Claims 1-11, 13, 21, 23-25, 30, 32-33, 36, and 38

1. Brief Description of Comerford

Comerford discloses a right to execute software that can be conditioned, manipulated, and/or transferred. (Ex. 1004, Comerford, 2:1-4, 17:25-30; Ex. 1001, Grimes Dec., at ¶ 110.) It discloses conditioning the right to execute "by a time period" and "based on the number of times it is invoked," but it also expressly provides that "the right to execute can be conditioned on any other parameter so long as it can be measured by the coprocessor to the satisfaction of the . . . software vendor." (Ex. 1004, Comerford, 2:23-34; Ex. 1001, Grimes Dec., at ¶ 110.) Comerford discloses three general objectives for conditioning the right to execute: (1) "a statement of the condition (or conditions) under which the application software may (or may not) be allowed to execute fully"; (2) "some objective criteria against which the condition or conditions can be measured"; and (3) "a software program which can test the conditions against the criteria and act in a way determined by results of that test." (Ex. 1004, Comerford, 3:7-17.) The conditions on the right to execute are "execution rights." (Ex. 1001, Grimes Dec., at ¶ 110.) Claim 9 of the '409 patent identifies "execution rights" as one example of "access control rights," and claim

8 recites that rules may "indicate access control rights." Accordingly, the conditions on the right to execute are rules. (*Id.*)

"[T]he criteria are stated . . . in the protected or encrypted portion of the application software." (Ex. 1004, Comerford, 3:22-25.) "[I]ncorporating the conditions of the right to execute within the protected software results in securing these conditions against alteration by the user or anyone else unless authorized by the software vendor." (*Id.* 3:30-34.) To further protect "the conditions which are tested against the programmed criteria," storage space in the non volatile memory of the coprocessor is used. (*See id.* 3:34-43, 3:50-54; Ex. 1001, Grimes Dec., at ¶ 111.) Additionally, Comerford discloses that "[t]he conditions of execution can be stored in the same file as the AK . . . ." (Ex. 1004, Comerford, 18:59-61.) "[E]ach time the protected application is run on the coprocessor 20, prior to authorizing execution, the application uses the criterion stated in the encrypted application file . . . and only authorizes execution in the event the criterion is met." (*Id.* 19:4-10.)

2. Comerford Incorporates the '629 Application by Reference

Comerford incorporates the '629 application by reference because it "discloses the basic software asset protection mechanism" that Comerford references. (*Id.* 17:25-30, 22:12-17.) The '629 application discloses a DRM solution applicable to software, and similar to what is disclosed in the '409 patent, computer hardware (i.e., a coprocessor) is used for controlling access to data. (Ex. 1001, Grimes Dec., at ¶ 112.) The disclosed invention is based on the concept that "software distribution techniques distribute to the user, in addition to the software itself, the right to execute that software." (Ex. 1005, '629 application, at 9.) It is this "right to execute" that is the focus of Comerford. (Ex. 1001, Grimes Dec., at ¶ 112.)

Software vendors partition software "into an encrypted portion P_e and an unencrypted (clear text) portion P_c" in order to protect their proprietary software. (*See* Ex. 1005, '629 application, at 10, 33.) This renders the software "inexecutable." (*Id.* at 28.) The "encrypted portion P_e" is the protected portion of the data recited in the claims. (Ex. 1001, Grimes Dec., at ¶ 113.) For the software to become executable, a "right to execute that software" must be installed on a "suitable coprocessor" associated with the host computer on which the user will run the software. (Ex. 1005, '629 application, at 9.)

The software is distributed "on magnetic media," "such as tape or floppy disk," or "via a communication link," such as a "telephone line, cable or broadcast transmission." (*Id.* at 10, 20.) This distribution of the protected portions of the data, using "magnetic media" or a "telephone line, cable or broadcast transmission," is open, as disclosed in the '409 patent and explained above, as it "us[es] mechanisms and media that are subject to access and copying." (Ex. 1001, Grimes Dec., at ¶ 114; Ex. 1002, '409 patent, 15:25-28, 32:57-61.) The right to execute—referenced elsewhere in the '629 application as RTE, Application Key, AK, and EAK (when encrypted)—may be distributed via the same means. (Ex. 1005, '629 application, at 11, 45.) Once the right to execute is installed, the coprocessor is able to decrypt and execute the encrypted portion of the software. (*Id.* at 15.) The coprocessor is "physically and logically secure." (*Id.* at 10.) "The logical and physical security of the coprocessor memory prevents the user from having access to [the] plaintext or executable form of the protected software." (*Id.* at 16.) "The protected part of the software is, thus, never exposed in plaintext form and never executed by unauthorized systems." (*Id.* at 10.) Like the '409 patent, Comerford discloses that "each and every access to an unprotected form of the protected portions of the data is limited in accordance with rules defining access rights to the data" because there is an access mechanism (i.e., the "physically and logically secure coprocessor") that decrypts and executes the encrypted portion, P_e, of the software if execution is authorized based on testing conditions against criteria that are associated with a conditioned "right-to-execute." (*See id.*; Ex. 1004, Comerford, 3:7-17, 4:11-39, 29:50-55; Ex. 1001, Grimes Dec., at ¶ 114.) This ensures that "[t]he protected part of the software is . . . **never** exposed in plaintext form and **never** executed by unauthorized systems." (Ex. 1005, '629 application, at 10 (emphasis added); Ex. 1001, Grimes Dec., at ¶ 114.) Also, like what is disclosed in the '409 patent, because the coprocessor operates as the access mechanism and the protected portion of the software "is partitioned into an encrypted portion P_e," "unauthorized access to the protected portions of the data is not to the unprotected form of the protected portions of the data." (Ex. 1001, Grimes Dec., at ¶ 114; Ex. 1005, '629 application, at 10.)

Because Comerford incorporates the '629 application by reference, the two, related disclosures are treated as a single, prior art reference. Invalidity by anticipation requires a single, prior art document that describes every element of the claimed invention, either expressly or inherently, but material not explicitly contained in that single, prior art document "may still be considered for purposes of anticipation if that material is incorporated by reference into the document." (*Advanced Display Sys., Inc. v. Kent State Univ.*, 212 F.3d 1272, 1282 (Fed. Cir. 2000).) "To incorporate material by reference, the host document must identify with detailed particularity what specific material it incorporates and clearly indicate where that material is found in the various documents." (*Id.*) Incorporation by reference is a question of law, and "the standard of one reasonably skilled in the art" is applied in making the incorporation-by-reference determination. (*Id.* at 1283.)

In addition to expressly incorporating the '629 application by reference as explained above, Comerford also includes several other references to the disclosure of the '629 application. (Ex. 1004, Comerford, 1:36-39, 1:65-2:1, 3:7-17, 3:25-30, 4:45-48, 5:54-61, 13:55-58, 15:17-20, 17:25-30, 17:35-40, 17:57-61, 18:4-8, 22:12-17, 27:10-17, 30:17-20.) Together, this is sufficiently particular for the '629 application to be incorporated by reference into Comerford. (*See* Ex. 1001, Grimes Dec., at ¶ 109.) The Federal Circuit has accepted much more general language. (*See, e.g.*, *Callaway Golf Co. v. Acushnet Co.*, 576 F.3d 1331, 1345-47 (Fed. Cir. 2009).)

3. Independent Claim 1

The claim chart below demonstrates in detail how Comerford anticipates claim 1. (Ex. 1001, Grimes Dec., at ¶ 115.)

1[a]. A method of	"[S]oftware can be distributed on magnetic media (such as tape or floppy disk) or by other means (telephone lines, cable or broadcast

distributing data, the method comprising:	transmission).” (*See, e.g.*, Ex. 1005, ’629 application, at 10.) “[T]he software may be distributed by any conventional technique.” (*See, e.g.*, *id.* at 43.) (*See, e.g.*, *id.* Fig. 5 (showing the “composite computing system” and “software distribution package”).)
[1b] protecting portions of the data; and	“The software is partitioned into an encrypted portion P_e and an unencrypted (clear text) portion P_c.” (*See, e.g.*, *id.* at 10.) “As distributed, of course, the protected software is inexecutable by the host computer since at least a portion is encrypted . . . .” (*See, e.g.*, *id.* at 28.) (*See also id.* at 55; Ex. 1001, Grimes Dec., at ¶ 115.)
[1c] openly distributing the protected portions of the data,	“[S]oftware can be distributed on magnetic media (such as tape or floppy disk) or by other means (telephone lines, cable or broadcast transmission).” (*See, e.g.*, Ex. 1005, ’629 application, at 10.) “[T]he method for transporting software . . . allows the software vendor to cryptographically hide some fraction of the software from the user in spite of the user being able to examine it with the resources available to him on the system.” (*See, e.g.*, *id.* at 31.) “[T]he software may be distributed by any conventional technique.” (*See, e.g.*, *id.* at 43.) (*See also id.* at 45; Ex. 1001, Grimes Dec., at ¶ 115.)
[1d] whereby each and every access to an unprotected form of the protected portions of the data is limited in accordance with rules defining access rights to the data as enforced by an access mechanism, so that	“[T]oday’s software distribution techniques distribute to the user, in addition to the software itself, the right to execute that software.” (*See, e.g.*, Ex. 1005, ’629 application, at 9.) “[I]t is only when the right to use is installed on the suitable coprocessor (which is associated with the host computer on which the user intends to run the software) that the software becomes executable.” (*See, e.g.*, *id.*) “The encrypted portion, P_e, of the software will be decrypted and executed by a physically and logically secure coprocessor if the coprocessor possesses the decryption key which embodies the right to execute. The protected part of the software is, thus, never exposed in plaintext form and never executed by unauthorized systems.” (*See, e.g.*, *id.* at 10.) “Whenever execution of the protected software is requested by the user, access is made, via the coprocessor’s second privilege level to the secure memory space to determine if the appropriate software decryption key is present; if present, the coprocessor initiates decryption of the protected software and storage of that software in the coprocessor’s first level secure memory space. . . . [I]f the necessary software decryption key is not present, the user’s request to execute the software is denied.” (*See, e.g.*, *id.* at 28-29.)

unauthorized access to the protected portions of the data is not to the unprotected form of the protected portions of the data.	“Because the coprocessor 15 is secure, the clear text protected software, although it resides in the memory of the coprocessor 15, is unavailable to the user or anyone else.” (*See, e.g.*, *id.* at 57.) “[T]he right to execute might be conditioned by a time period . . . or it could be conditioned based on the number of times it is invoked . . . . [T]he right to execute can be conditioned on any other parameter so long as it can be measured by the coprocessor to the satisfaction of the source of that right to execute (the software vendor).” (*See, e.g.*, Ex. 1004, Comerford, 2:24-34.) “In order to condition the right to execute . . . there must be: 1) a statement of the condition (or conditions) under which the application software may (or may not) be allowed to execute fully, and 2) some objective criteria against which the condition or conditions can be measured, and 3) a software program which can test the conditions against the criteria and act in a way determined by results of that test.” (*See, e.g.*, *id.* 3:7-17.) “Whenever the protected software is run, the decryption key and the terminal date are accessed from the coprocessor's non-volatile memory. The criterion tested in the protected software requires that the terminal date be compared to the current date; if the current date is beyond the terminal date, then execution of the protected software does not proceed. . . . It should be apparent to those skilled in the art that another condition which can be substituted for the terminal date condition is the number of times the software is executed. . . . It should be apparent that there are many variations to these specific implementations, including elapsed time, passwords, and combinations of these and other measurables, all of which are within the scope of the invention.” (*See, e.g.*, *id.* 4:11-39.) “The flag settings for this particular AK include settings that allow it to be backed up and do not allow it to be moved or erased. . . . . . . An AK installation which proceeded under conditions as described above would allow a person to acquire the right to execute a piece of software for demonstration purposes, typically a one time use. . . . The software vendor is protected from having his code reinstalled repeatedly, using demonstration software, without control.” (*See, e.g.*, *id.* 16:43-60.) “Associated with each key are a number of binary flags, a bit for each of the following: Meta, Condition, Erase, Transfer and Backup. It should be understood that this list is a useful subset of such flags and that the set would almost certainly be extended by one skilled in the art.” (*See, e.g.*, *id.* 29:25-30.) “One of the multibyte entries is headed ‘Condition’ and this field includes

	the data associated with a conditioned key, and thus keys AK3 and AKn include data in that field which can be tested by criteria stored in the application they decrypt to determine if execution is authorized." (*See, e.g.*, *id.* 29:50-55.) (*See, e.g.*, *id.* Figs. 2, 3, 4, 19 (showing "conditioned rights-to-execute" and "coprocessor 20").) (*See also* Ex. 1005, '629 application, at 13, 37, 57; Ex. 1006, Chandra, 5:24-30; Ex. 1001, Grimes Dec., at ¶ 115.)

4. Claims 2-11 and 13, Which Depend From Claim 1

Claim 2 depends from claim 1 and further recites: "wherein the protecting of portions of the data comprises encrypting the portions of the data, whereby unauthorized access to the protected data is not to the un-encrypted form of the protected data." Comerford discloses partitioning software "into an encrypted portion P_e and an unencrypted (clear text) portion P_c." (Ex. 1005, '629 application, at 10.) "The encrypted portion, P_e, of the software will be decrypted and executed by a physically and logically secure coprocessor if the coprocessor possesses the decryption key which embodies the right to execute. The protected part of the software is, thus, never exposed in plaintext form and never executed by unauthorized systems." (*Id.*) As discussed above, Comerford discloses this additional limitation in a similar manner to what is disclosed in the '409 patent. (Ex. 1001, Grimes Dec., at ¶ 116.) Because the coprocessor operates as the access mechanism and the protected portion of the software "is partitioned into an encrypted portion P_e," "unauthorized access to the protected data is not to the un-encrypted form of the protected data." (Ex.

1001, Grimes Dec., at ¶ 116; Ex. 1005, ’629 application, at 10.) Thus, Comerford anticipates claim 2. (Ex. 1001, Grimes Dec., at ¶ 116.)

Claim 3 depends from claim 2 and further recites: “wherein the encrypting of portions of the data encrypts the portions of the data with a data encrypting key, the data encrypting key having a corresponding data decrypting key.” Comerford discloses an “encryption key (AK) used to encrypt the software” and a “decryption key AK needed to render the encrypted software executable.” (Ex. 1005, ’629 application, at 13-14.) This is a symmetric-key cryptosystem in which the same key is used for encryption and decryption of the data. (*See id.* at 33-34; Ex. 1001, Grimes Dec., at ¶ 117.) Because the keys are the same, the data decrypting key corresponds to the data encrypting key. (Ex. 1001, Grimes Dec., at ¶ 117.) Claim 3 also recites “encrypting the data encrypting key,” and Comerford discloses that AK, which is both the data encrypting key and the data decrypting key, is provided to the coprocessor in encrypted form as EAK. (*Id.* at ¶ 118; *e.g.*, Ex. 1005, ’629 application, at 11.) The additional disclosures in the claim charts below demonstrate in detail how Comerford anticipates claims 2 and 3. (Ex. 1001, Grimes Dec., at ¶ 119.)

2. A method as in claim 1, wherein the protecting of portions of the data comprises encrypting the portions of the data, whereby unauthorized access to the protected data is not to the un-encrypted form of the protected data.	“The software is partitioned into an encrypted portion P_e and an unencrypted (clear text) portion P_c. . . . The encrypted portion, P_e, of the software will be decrypted and executed by a physically and logically secure coprocessor if the coprocessor possesses the decryption key which embodies the right to execute. The protected part of the software is, thus, never exposed in plaintext form and never executed by unauthorized systems.” (*See, e.g.*, Ex. 1005, ’629 application, at 10.)

3[a]. A method as in claim 2, wherein the encrypting of portions of the data encrypts the portions of the data with a data encrypting key, the data encrypting key having a corresponding data decrypting key,	"[T]hat medium which is ready to be sold or released may consist of the following (see Fig. 3): 1. An application which consists of at least one file of program encrypted with a key AK selected by the software vendor. 2. The decryption key AK needed to render the encrypted software executable provided in encrypted form EAK where the encryption is by the hardware vendor's (secret) encryption key CSK." (*See, e.g.*, Ex. 1005, '629 application, at 33-34.) "The software vendor . . . uses his own (secret) encryption key AK to encrypt the token data as well as critical parts (part 2) of the application software." (*See, e.g.*, *id.* at 55.) "Upon successful completion of the ARE process, the software decryption key AK, received by the coprocessor 15 in encrypted form E_{CSK}(AK) has been decrypted, and in response to successful completion of the ARE, AK has been transferred (5) to the permanent memory 15P of the coprocessor 15." (*See, e.g.*, *id.* at 57.)
[3b] the method further comprising: encrypting the data encrypting key.	"This part of the application software is encrypted with a key (AK) provided by the software vendor. The software key (AK) is supplied to the user in encrypted form (EAK), encrypted under a key (CSK) known only to the hardware vendor." (*See, e.g.*, *id.* at 33.)

Claim 4 depends from claim 3 and further recites: "providing a decrypting key corresponding to the key encrypting key." Comerford discloses encrypting AK using a key "selected from a list of Coprocessor Supervisor Keys (CSKs) . . . stored in all coprocessors supplied by a given vendor." (Ex. 1005, '629 application, at 11.) "The coprocessor accepts the encrypted software key EAK . . . and decrypts it using a coprocessor supervisor key CSK stored in the coprocessor at the time of manufacture." (*Id.* at 22.) Therefore, the coprocessor is provided with a decrypting key corresponding to the key encrypting key, and Comerford anticipates claim 4. (Ex. 1001, Grimes Dec., at ¶ 120.) The additional disclosures in the claim chart below demonstrate in detail how Comerford anticipates claim 4. (Ex. 1001, Grimes Dec., at ¶ 121.)

4. A method as in claim 3, further comprising: providing a decrypting key corresponding to the key encrypting key.	“[T]he key used to encrypt the AK is selected from a list of Coprocessor Supervisor Keys (CSKs) which is stored in all coprocessors supplied by a given vendor.” (Ex. 1005, ’629 application, at 11.) “The coprocessor accepts the encrypted software key EAK . . . and decrypts it using a coprocessor supervisor key CSK stored in the coprocessor at the time of manufacture.” (*See, e.g.*, *id.* at 22.)

Claim 5 depends from claim 1 and further recites: “wherein the data represent at least one of software, text, numbers, graphics, audio, and video.” Comerford discloses “a software copy protection mechanism.” (Ex. 1004, Comerford, 1:12-13.) Accordingly, Comerford anticipates claim 5 as detailed in the claim chart below. (Ex. 1001, Grimes Dec., at ¶¶ 122-123.)

5. A method as in claim 1, wherein the data represent at least one of software, text, numbers, graphics, audio, and video.	“The invention is in the field of data processing, especially in connection with a software copy protection mechanism.” (*See, e.g.*, Ex. 1004, Comerford, 1:11-13.)

Claims 6-8 depend from claim 1, and each adds an additional limitation regarding the “rules” of claim 1. (Ex. 1001, Grimes Dec., at ¶¶ 124, 126, 128.) Comerford discloses that software only becomes executable “when [a] right [to execute] is installed on [a] suitable coprocessor (which is associated with the host computer on which the user intends to run the software).” (Ex. 1005, ’629 application, at 9.) Additionally, Comerford discloses that the right to execute may be conditioned, and each time a user tries to run the protected software, a software program tests the conditions against the criteria and “only authorizes execution in the event the criterion is met." (*See, e.g.*, Ex. 1004, Comerford, 3:7-17, 4:8-39, 19:4-10; Ex. 1001, Grimes Dec., at ¶ 124.) Therefore, Comerford discloses rules that indicate which users are allowed to access the protected portions of the data. (Ex. 1001, Grimes Dec., at ¶ 124.)

A conditioned right to execute indicates distribution rights of the data because the only users that can decrypt and execute the protected software are those users who satisfy the specified conditions. (Ex. 1001, Grimes Dec., at ¶ 126; *see, e.g.*, Ex. 1004, Comerford, 4:11-39.) Additionally, Comerford discloses a demonstration-software embodiment in which flag settings are used by the software vendor to "protect[] from having his code reinstalled repeatedly . . . without control." (*See* Ex. 1004, Comerford, 16:33-60.)

Comerford discloses access control rights of the user because it discloses conditions on the right to execute that are execution rights, which constitute access control rights of the user. (Ex. 1001, Grimes Dec., at ¶ 128.) The additional disclosures detailed in the claim charts below demonstrate how Comerford anticipates claims 6-8. (Ex. 1001, Grimes Dec., at ¶¶ 124-129.)

6[a]. A method as in claim 1, wherein the rules indicate which users are allowed to access the protected portions of the data,	"[I]t is only when the right to use is installed on the suitable coprocessor (which is associated with the host computer on which the user intends to run the software) that the software becomes executable." (*See, e.g.*, Ex. 1005, '629 application, at 9.) "The encrypted portion, P_e, of the software will be decrypted and executed by a physically and logically secure coprocessor if the coprocessor possesses the decryption key which embodies the right to execute. The protected part of the software is, thus, never exposed in plaintext form and never executed by unauthorized systems." (*See, e.g.*, *id.* at 10.)

	"[T]he right to execute might be conditioned by a time period . . . or it could be conditioned based on the number of times it is invoked . . . . [T]he right to execute can be conditioned on any other parameter so long as it can be measured by the coprocessor to the satisfaction of the source of that right to execute (the software vendor)." (*See, e.g.*, Ex. 1004, Comerford, 2:24-34.) "In order to condition the right to execute . . . there must be: 1) a statement of the condition (or conditions) under which the application software may (or may not) be allowed to execute fully, and 2) some objective criteria against which the condition or conditions can be measured, and 3) a software program which can test the conditions against the criteria and act in a way determined by results of that test." (*See, e.g.*, *id.* 3:7-17.) "The criterion tested in the protected software requires that the terminal date be compared to the current date; if the current date is beyond the terminal date, then execution of the protected software does not proceed. . . . It should be apparent to those skilled in the art that another condition which can be substituted for the terminal date condition is the number of times the software is executed. . . . It should be apparent that there are many variations to these specific implementations, including elapsed time, passwords, and combinations of these and other measurables, all of which are within the scope of the invention." (*See, e.g.*, *id.* 4:14-39.) "An AK installation which proceeded under conditions as described above would allow a person to acquire the right to execute a piece of software for demonstration purposes, typically a one time use. . . . The software vendor is protected from having his code reinstalled repeatedly, using demonstration software, without control." (*See, e.g.*, *id.* 16:49-60.)
[6b] the method further comprising allowing the user access to the unprotected form of a protected portion of the data only if the rules indicate that the user is	This limitation is substantially similar to limitation 1d, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1004, Comerford, 2:24-34, 3:7-17, 4:11-39, 16:43-60, 29:25-30, 29:50-55, Figs. 2, 3, 4, 19; Ex. 1005, '629 application, at 9-10, 28-29, 57; *see also* Ex. 1005, '629 application, at 13, 37, 57; Ex. 1006, Chandra, 5:24-30.)

allowed to access that portion of the data.	

7[a]. A method as in claim 1 wherein the rules indicate distribution rights of the data,	"[I]t is only when the right to use is installed on the suitable coprocessor (which is associated with the host computer on which the user intends to run the software) that the software becomes executable." (*See, e.g.*, Ex. 1005, '629 application, at 9.) "[I]t is the encrypted fraction of the software which will be protected from redistribution by the user." (*See, e.g.*, *id.* at 33.) "In order to condition the right to execute . . . there must be: 1) a statement of the condition (or conditions) under which the application software may (or may not) be allowed to execute fully, and 2) some objective criteria against which the condition or conditions can be measured, and 3) a software program which can test the conditions against the criteria and act in a way determined by results of that test." (*See, e.g.*, Ex. 1004, Comerford, 3:7-17.) "The criterion tested in the protected software requires that the terminal date be compared to the current date; if the current date is beyond the terminal date, then execution of the protected software does not proceed. . . . It should be apparent to those skilled in the art that another condition which can be substituted for the terminal date condition is the number of times the software is executed. . . . It should be apparent that there are many variations to these specific implementations, including elapsed time, passwords, and combinations of these and other measurables, all of which are within the scope of the invention." (*See, e.g.*, *id.* 4:14-39.) "The flag settings for this particular AK include settings that allow it to be backed up and do not allow it to be moved or erased. . . . An AK installation which proceeded under conditions as described above would allow a person to acquire the right to execute a piece of software for demonstration purposes, typically a one time use. . . . The software vendor is protected from having his code reinstalled repeatedly, using demonstration software, without control." (*See, e.g.*, *id.* 16:43-

	60.) “Associated with each key are a number of binary flags, a bit for each of the following: Meta, Condition, Erase, Transfer and Backup. It should be understood that this list is a useful subset of such flags and that the set would almost certainly be extended by one skilled in the art.” (*See, e.g.*, *id.* 29:25-30.)
[7b] the method further comprising: allowing distribution of the unprotected form of the protected data portions only in accordance with the distribution rights indicated in the rules.	This limitation is substantially similar to limitation 1d, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1004, Comerford, 2:24-34, 3:7-17, 4:11-39, 16:43-60, 29:25-30, 29:50-55, Figs. 2, 3, 4, 19; Ex. 1005, ’629 application, at 9-10, 28-29, 57; *see also* Ex. 1005, ’629 application, at 13, 37, 57; Ex. 1006, Chandra, 5:24-30.)

8[a]. A method as in claim 1, wherein the rules indicate access control rights of the user,	“[I]t is only when the right to use is installed on the suitable coprocessor (which is associated with the host computer on which the user intends to run the software) that the software becomes executable.” (*See, e.g.*, Ex. 1005, ’629 application, at 9.) “[T]he right to execute might be conditioned by a time period . . . or it could be conditioned based on the number of times it is invoked . . . . [T]he right to execute can be conditioned on any other parameter so long as it can be measured by the coprocessor to the satisfaction of the source of that right to execute (the software vendor).” (*See, e.g.*, Ex. 1004, Comerford, 2:24-34.) “In order to condition the right to execute . . . there must be: 1) a statement of the condition (or conditions) under which the application software may (or may not) be allowed to execute fully, and 2) some objective criteria against which the condition or conditions can be measured, and 3) a software program which can test the conditions against the criteria and act in a way determined by results of that test.” (*See, e.g.*, *id.* 3:7-17.) “The criterion tested in the protected software requires that the terminal date be compared to the current date; if the current date is beyond the terminal date, then execution of the protected software does not proceed. . . . It should be apparent to those skilled in the art that another condition which can be substituted for the terminal date

	condition is the number of times the software is executed. . . . It should be apparent that there are many variations to these specific implementations, including elapsed time, passwords, and combinations of these and other measurables, all of which are within the scope of the invention." (*See, e.g.*, *id.* 4:14-39.) "The flag settings for this particular AK include settings that allow it to be backed up and do not allow it to be moved or erased. . . . An AK installation which proceeded under conditions as described above would allow a person to acquire the right to execute a piece of software for demonstration purposes, typically a one time use. . . . The software vendor is protected from having his code reinstalled repeatedly, using demonstration software, without control." (*See, e.g.*, *id.* 16:43-60.) "Associated with each key are a number of binary flags, a bit for each of the following: Meta, Condition, Erase, Transfer and Backup. It should be understood that this list is a useful subset of such flags and that the set would almost certainly be extended by one skilled in the art." (*See, e.g.*, *id.* 29:25-30.) "One of the multibyte entries is headed 'Condition' and this field includes the data associated with a conditioned key, and thus keys AK3 and AKn include data in that field which can be tested by criteria stored in the application they decrypt to determine if execution is authorized." (*See, e.g.*, *id.* 29:50-55.)
[8b] the method further comprising: allowing the user to access the unprotected form of the protected data portions only in accordance with the access control rights indicated in the rules.	This limitation is substantially similar to limitation 1d, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1004, Comerford, 2:24-34, 3:7-17, 4:11-39, 16:43-60, 29:25-30, 29:50-55, Figs. 2, 3, 4, 19; Ex. 1005, '629 application, at 9-10, 28-29, 57; *see also* Ex. 1005, '629 application, at 13, 37, 57; Ex. 1006, Chandra, 5:24-30.)

Claim 9 depends from claim 8 and further recites: "wherein the access control rights include at least one of: local display rights, printing rights, copying rights, execution rights, transmission rights, and modification rights." Comerford satisfies this limitation because it discloses conditions on the right to execute that are execution rights. (Ex. 1001, Grimes Dec., at ¶ 130.) This is detailed with respect to claim 8, so only pinpoint citations are provided in the claim chart below, which demonstrates in detail how Comerford anticipates claim 9. (*Id.* at ¶¶ 130-131.)

9. A method as in claim 8, wherein the access control rights include at least one of: local display rights, printing rights, copying rights, execution rights, transmission rights, and modification rights.	This limitation is substantially similar to limitation 8a, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1004, Comerford, 2:24-34, 3:7-17, 4:14-39, 16:43-60, 29:25-30, 29:50-55; Ex. 1005, '629 application, at 9.)

Claim 10 depends from claim 1 and further recites that "the rules indicate access control quantities." The '409 patent provides examples of access control quantities, such as a "[n]umber of read-accesses" and an "[e]xpiration date." (*E.g.*, Ex. 1002, '409 patent, 25:32-50.) Comerford discloses "terminal dates and times," which define an expiration date, and a "number of executions," which is the software-execution equivalent of a number of read-accesses, and thus, Comerford discloses this limitation. (Ex. 1001, Grimes Dec., at ¶ 132.) The additional disclosures in the claim chart below demonstrate how Comerford anticipates claim 10. (*Id.* at ¶¶ 132-133.)

10[a]. A method as in claim 1, wherein the rules indicate access control quantities,	"[T]he right to execute might be conditioned by a time period (a right to execute which exists up until a cut-off date and/or time) or it could be conditioned based on the number of times it is invoked (for example the vendor could sell a user the right to execute the protected application ten times)." (*See, e.g.*, Ex. 1004, Comerford, 2:24-30.)

	(*See also id* 4:11-39; Ex. 1001, Grimes Dec., at ¶ 133.)
[10b] the method further comprising: allowing access to the unprotected form of the protected data portions only in accordance with the access control quantities indicated in the rules.	This limitation is substantially similar to limitation 1d, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1004, Comerford, 2:24-34, 3:7-17, 4:11-39, 16:43-60, 29:25-30, 29:50-55, Figs. 2, 3, 4, 19; Ex. 1005, ’629 application, at 9-10, 28-29, 57; *see also* Ex. 1005, ’629 application, at 13, 37, 57; Ex. 1006, Chandra, 5:24-30.)

Claim 11 depends from claim 10 and further recites: “wherein the access control quantities include at least one of: a number of allowed read-accesses to the data; an allowable size of a read-access to the data; an expiration date of the data; an intensity of accesses to the data; an allowed level of accuracy and fidelity; and an allowed resolution of access to the data.” Comerford discloses access control quantities of this sort, including “terminal dates and times,” which equate to an expiration date of the data; and, “numbers of executions,” which is the software-execution equivalent of “a number of allowed read-accesses.” (*See* Ex. 1004, Comerford, 2:24-30, 4:11-39; Ex. 1001, Grimes Dec., at ¶ 134.) Accordingly, Comerford anticipates claim 11 as detailed in the claim chart below. (Ex. 1001, Grimes Dec., at ¶¶ 134-135.)

11. A method as in claim 10, wherein the access control quantities include at least one of: a number of allowed read-accesses to the data; an allowable size of a read-access to the data; an expiration date of the data; an intensity of accesses to the data; an allowed level of accuracy and fidelity; and an allowed resolution of access to the data.	This limitation is disclosed by the disclosure from Comerford that is detailed in full for limitation 10a above. (*See, e.g.*, Ex. 1004, Comerford, 2:24-30; *see also id.* 4:11-39.)

Claim 13 depends from claim 1 and further recites: “wherein the rules relate to at least one of: characteristics of users; characteristics of protected data; and environmental characteristics.” Comerford’s disclosure of conditions on the right to execute satisfies this limitation because the right to execute can be conditioned on any parameter “so long as it can be measured by the coprocessor to the satisfaction of the source of that right to execute (the software vendor).” (Ex. 1001, Grimes Dec., at ¶ 136; Ex. 1004, Comerford, 2:30-34.) Thus, the conditions (i.e., rules) can “relate to at least one of: characteristics of users; characteristics of protected data; and environmental characteristics.” (Ex. 1001, Grimes Dec., at ¶ 136.) Further, Comerford specifically identifies certain conditions, such as “a time period” and “the number of times it is invoked,” that satisfy this limitation. (*Id.*; Ex. 1004, Comerford, 2:24-30.) The additional disclosures in the claim chart below demonstrate how Comerford anticipates claim 13. (Ex. 1001, Grimes Dec., at ¶ 137.)

13. A method as in claim 1, wherein the rules relate to at least one of: characteristics of users; characteristics of protected data; and environmental characteristi	“[I]t is only when the right to use is installed on the suitable coprocessor (which is associated with the host computer on which the user intends to run the software) that the software becomes executable.” (*See, e.g.*, Ex. 1005, ’629 application, at 9.) “[T]he right to execute might be conditioned by a time period . . . or it could be conditioned based on the number of times it is invoked . . . . [T]he right to execute can be conditioned on any other parameter so long as it can be measured by the coprocessor to the satisfaction of the source of that right to execute (the software vendor).” (*See, e.g.*, Ex. 1004, Comerford, 2:24-34.) “In order to condition the right to execute . . . there must be: 1) a statement of the condition (or conditions) under which the application software may (or may not) be allowed to execute fully, and 2) some objective criteria against which the condition or conditions can be measured, and 3) a software program which can test the conditions against the criteria and

cs.	act in a way determined by results of that test." (*See, e.g.*, *id.* 3:7-17.) "The criterion tested in the protected software requires that the terminal date be compared to the current date; if the current date is beyond the terminal date, then execution of the protected software does not proceed. . . . It should be apparent to those skilled in the art that another condition which can be substituted for the terminal date condition is the number of times the software is executed. . . . It should be apparent that there are many variations to these specific implementations, including elapsed time, passwords, and combinations of these and other measurables, all of which are within the scope of the invention." (*See, e.g.*, *id.* 4:14-39.) (*See, e.g.*, *id.* Figs. 2, 3, 4, 19 (showing "conditioned rights-to-execute").) (*See also id.* 3:22-25, 18:59-61; Ex. 1001, Grimes Dec., at ¶ 137.)

5. Independent Claims 21, 23-25, 30, 32-33, 36, and 38

The limitations of claim 21 are similar to those in claim 1, but claim 21 also recites "protecting rules defining access rights to the data" and "openly distributing the protected portions of the data and the protected rules." (Ex. 1001, Grimes Dec., at ¶ 139.) Comerford discloses conditions on the right to execute (i.e., rules). (*Id.*) The criteria and conditions are secured "in the protected or encrypted portion of the application software." (*Id.*; *see* Ex. 1004, Comerford, 3:22-34.) "[I]ncorporating the conditions of the right to execute within the protected software results in securing these conditions against alteration by the user or anyone else unless authorized by the software vendor." (Ex. 1004, Comerford, 3:30-34.) These rules are distributed along with the protected software. (Ex. 1001, Grimes Dec., at ¶ 139.) The claim chart below demonstrates in detail how Comerford anticipates claim 21. (*Id.* at ¶¶ 139-140.)

21[a]. A method of	(*See, e.g.*, Ex. 1005, '629 application, Fig. 5 (showing the

distributing data for subsequent controlled use of the data by a user, the method comprising:	“composite computing system” and “software distribution package”).) (*See, e.g.*, Ex. 1004, Comerford, Fig. 19 (showing “a collection of rights to execute”).)
[21b] protecting portions of the data;	This limitation is substantially similar to limitation 1b, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1005, ’629 application, at 10, 28; *see also id.* at 55.)
[21c] protecting rules defining access rights to the data; and	“This part of the application software is encrypted with a key (AK) provided by the software vendor. The software key (AK) is supplied to the user in encrypted form (EAK), encrypted under a key (CSK) known only to the hardware vendor.” (*See, e.g.*, *id.* at 33.) “[T]he right to execute might be conditioned by a time period . . . or it could be conditioned based on the number of times it is invoked . . . . [T]he right to execute can be conditioned on any other parameter so long as it can be measured by the coprocessor to the satisfaction of the source of that right to execute (the software vendor).” (*See, e.g.*, Ex. 1004, Comerford, 2:24-34.) “In order to condition the right to execute . . . there must be: 1) a statement of the condition (or conditions) under which the application software may (or may not) be allowed to execute fully, and 2) some objective criteria against which the condition or conditions can be measured, and 3) a software program which can test the conditions against the criteria and act in a way determined by results of that test.” (*See, e.g.*, *id.* 3:7-17.) “[T]he criteria are stated in software, and more particularly, in the protected or encrypted portion of the application software. As is described in our copending application Ser. No. 927,629, the only form in which application software is available to the user is in encrypted form; because the user does not have access to the decryption key as a data object, he is unable to modify, or even read the protected software. Thus, incorporating the conditions of the right to execute within the protected software results in securing these conditions against alteration by the user or anyone else unless authorized by the software vendor.” (*See, e.g.*, *id.*

	3:23-34.) "The conditions of execution can be stored in the same file as the AK and can be installed at the same time as AK." (*See, e.g.*, *id.* 18:59-61.) "[E]ach time the protected application is run on the coprocessor 20, prior to authorizing execution, the application uses the criterion stated in the encrypted application file . . . ." (*See, e.g.*, *id.* 19:4-10.) "Associated with each key are a number of binary flags, a bit for each of the following: Meta, Condition, Erase, Transfer and Backup. It should be understood that this list is a useful subset of such flags and that the set would almost certainly be extended by one skilled in the art." (*See, e.g.*, *id.* 29:25-30.) "One of the multibyte entries is headed 'Condition' and this field includes the data associated with a conditioned key, and thus keys AK3 and AKn include data in that field which can be tested by criteria stored in the application they decrypt to determine if execution is authorized." (*See, e.g.*, *id.* 29:50-55.) (*See, e.g.*, *id.* Figs. 2, 3, 4, 19 (showing showing "conditioned rights-to-execute" and "distribution disk 16").) (*See also* Ex. 1005, '629 application, at 55; Ex. 1004, Comerford, 4:11-39, 16:33-60; Ex. 1001, Grimes Dec., at ¶ 140.)
[21d] openly distributing the protected portions of the data and the protected rules, whereby	"[S]oftware can be distributed on magnetic media (such as tape or floppy disk) or by other means (telephone lines, cable or broadcast transmission)." (*See, e.g.*, Ex. 1005, '629 application, at 10.) "The software vendor supplied key (AK) is made available to the coprocessor by supplying it, in encrypted form, with the program via the software distribution medium or other means as described in the case of the ETD." (*See, e.g.*, *id.* at 11.) "[T]he method for transporting software . . . allows the software vendor to cryptographically hide some fraction of the software from the user in spite of the user being able to examine it with the resources available to him on the system." (*See, e.g.*, *id.* at 31.) "[T]he software may be distributed by any conventional technique." (*See, e.g.*, *id.* at 43.) "As shown in Fig. 3 the three files may be distributed as unit . . . . A first file is an encrypted software decryption key EAK. The second file is the software which includes both plain text software (PART 1) and protected or encrypted software (PART 2) (EAK

	(Software, Part 2)).” (*See, e.g.*, *id.* at 45.)
[21e] controlled access to an unprotected form of the protected portions of the data is provided only in accordance with the rules as enforced by an access mechanism, so that unauthorized access to the protected portions of the data is not to the unprotected form of the protected portions of the data.	This limitation is substantially similar to limitation 1d, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1004, Comerford, 2:24-34, 3:7-17, 4:11-39, 16:43-60, 29:25-30, 29:50-55, Figs. 2, 3, 4, 19; Ex. 1005, ’629 application, at 9-10, 28-29, 57; *see also* Ex. 1005, ’629 application, at 13, 37, 57; Ex. 1006, Chandra, 5:24-30.)

The limitations of claim 23 are similar to those in claim 21, but claim 23 also recites “limiting transmission of the protected portions of the data from the device (a) only as protected data or (b) in accordance with the rules as enforced by the access mechanism.” (Ex. 1001, Grimes Dec., at ¶ 141.) Comerford satisfies this limitation because it discloses that “the encrypted fraction of the software . . . will be protected from redistribution by the user.” (Ex. 1005, ’629 application, at 33; Ex. 1001, Grimes Dec., at ¶ 141.) “The user can make as many ‘backup’ copies of the software as he desires; however without access to a logically and physically secure coprocessor storing the decryption key AK, any ‘backup’ copies of the software are unusable since the encrypted portion of the software cannot be decrypted.” (Ex. 1005, ’629 application, at 16.) Additionally, Comerford discloses conditions on the right to execute (i.e., rules) that are enforced by the secure coprocessor. (Ex. 1001, Grimes Dec., at ¶ 141.) Comerford's disclosure of conditions on the right to execute satisfies this limitation because the right to execute can be conditioned on any parameter "so long as it can be measured by the coprocessor to the satisfaction of the source of that right to execute (the software vendor)," and, thus, the parameters may be used to limit transmission of the protected portions of the data. (*Id.*; Ex. 1004, Comerford, 2:30-34.) The claim chart below demonstrates in detail how Comerford anticipates claim 23. (Ex. 1001, Grimes Dec., at ¶¶ 141-142.)

23[a]. A method of controlling secondary distribution of data, the method comprising:	(*See, e.g.*, Ex. 1005, '629 application, Fig. 5 (showing the "composite computing system" and "software distribution package").) (*See, e.g.*, Ex. 1004, Comerford, Fig. 19 (showing "a collection of rights to execute").)
[23b] protecting portions of the data;	This limitation is substantially similar to limitation 1b, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1005, '629 application, at 10, 28; *see also id.* at 55.)
[23c] protecting rules defining access rights to the data;	This limitation is substantially similar to limitation 21c, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1004, Comerford, 2:24-34, 3:7-17, 3:23-34, 18:59-61, 19:4-10, 29:25-30, 29:50-55, Figs. 2, 3, 4, 19; Ex. 1005, '629 application, at 33; *see also* Ex. 1004, Comerford, 4:11-39, 16:33-60; Ex. 1005, '629 application, at 55.)
[23d] openly providing the protected portions of the data and the protected rules to a device having an access	"[S]oftware can be distributed on magnetic media (such as tape or floppy disk) or by other means (telephone lines, cable or broadcast transmission)." (*See, e.g.*, Ex. 1005, '629 application, at 10.) "The encrypted portion, P_e, of the software will be decrypted and executed by a physically and logically secure coprocessor if the coprocessor possesses the decryption key which embodies the right to execute." (*See, e.g.*, *id.*) "The software vendor supplied key (AK) is made available to the coprocessor by supplying it, in encrypted form, with the program via the

mechanism; and	software distribution medium or other means as described in the case of the ETD." (*See, e.g.*, *id.* at 11.) "The coprocessor accepts the encrypted software key EAK from either the token cartridge or the software distribution media (preferred) and decrypts it using a coprocessor supervisor key CSK stored in the coprocessor at the time of manufacture." (*See, e.g.*, *id.* at 22.) "[T]he method for transporting software . . . allows the software vendor to cryptographically hide some fraction of the software from the user in spite of the user being able to examine it with the resources available to him on the system." (*See, e.g.*, *id.* at 31.) "[T]he software may be distributed by any conventional technique." (*See, e.g.*, *id.* at 43.) "As shown in Fig. 3 the three files may be distributed as unit . . . . A first file is an encrypted software decryption key EAK. The second file is the software which includes both plain text software (PART 1) and protected or encrypted software (PART 2) (EAK (Software, Part 2))." (*See, e.g.*, *id.* at 45.)
[23e] limiting transmission of the protected portions of the data from the device (a) only as protected data or (b) in accordance with the rules as enforced by the access mechanism, so that unauthorized access to the protected portions of the data is not to an unprotected form of the protected portions of the	"The user can make as many 'backup' copies of the software as he desires; however without access to a logically and physically secure coprocessor storing the decryption key AK, any 'backup' copies of the software are unusable since the encrypted portion of the software cannot be decrypted." (*See, e.g.*, *id.* at 16.) "[I]t is the encrypted fraction of the software which will be protected from redistribution by the user." (*See, e.g.*, *id.* at 33.) "In order to condition the right to execute . . . there must be: 1) a statement of the condition (or conditions) under which the application software may (or may not) be allowed to execute fully, and 2) some objective criteria against which the condition or conditions can be measured, and 3) a software program which can test the conditions against the criteria and act in a way determined by results of that test." (*See, e.g.*, Ex. 1004, Comerford, 3:7-17.) "The flag settings for this particular AK include settings that allow it to be backed up and do not allow it to be moved or erased. . . . An AK installation which proceeded under conditions as described above would allow a person to acquire the right to execute a piece of software for demonstration purposes, typically a one time use. . . . The software vendor is protected from having his code reinstalled repeatedly, using demonstration software, without control." (*See, e.g.*, *id.* 16:43-60.) "Associated with each key are a number of binary flags, a bit for each of

data.	the following: Meta, Condition, Erase, Transfer and Backup. It should be understood that this list is a useful subset of such flags and that the set would almost certainly be extended by one skilled in the art." (*See, e.g.*, *id.* 29:25-30.) (*See also* Ex. 1004, Comerford, 4:11-39; Ex. 1001, Grimes Dec., at ¶ 142.)

The limitations of claim 24 are similar to those in previous claims, but claim 24 is drafted from the recipient's perspective instead of the distributor's perspective. (Ex. 1001, Grimes Dec., at ¶ 143.) The claim chart below demonstrates in detail how Comerford anticipates claim 24. (Ex. 1001, Grimes Dec., at ¶¶ 143-144.)

24[a]. A method of accessing openly distributed data, the method comprising:	(*See, e.g.*, Ex. 1005, '629 application, Fig. 5 (showing the "composite computing system" and "software distribution package").) (*See, e.g.*, Ex. 1004, Comerford, Fig. 19 (showing "a collection of rights to execute").)
[24b] obtaining openly distributed data having protected data portions and rules defining access rights to the protected data portions; and	"[S]oftware can be distributed on magnetic media (such as tape or floppy disk) or by other means (telephone lines, cable or broadcast transmission). The software is partitioned into an encrypted portion P_e and an unencrypted (clear text) portion P_c. . . . The encrypted portion, P_e, of the software will be decrypted and executed by a physically and logically secure coprocessor if the coprocessor possesses the decryption key which embodies the right to execute." (*See, e.g.*, Ex. 1005, '629 application, at 10.) "The coprocessor accepts the encrypted software key EAK from either the token cartridge or the software distribution media (preferred) and decrypts it using a coprocessor supervisor key CSK stored in the coprocessor at the time of manufacture." (*See, e.g.*, *id.* at 22.) "[T]he method for transporting software . . . allows the software vendor to cryptographically hide some fraction of the software from the user in spite of the user being able to examine it with the resources available to him on the system." (*See, e.g.*, *id.* at 31.) "[T]he software may be distributed by any conventional technique." (*See, e.g.*, *id.* at 43.)

	“As shown in Fig. 3 the three files may be distributed as unit . . . . A first file is an encrypted software decryption key EAK. The second file is the software which includes both plain text software (PART 1) and protected or encrypted software (PART 2) (EAK (Software, Part 2)).” (*See, e.g.*, *id.* at 45.) “[T]he right to execute might be conditioned by a time period . . . or it could be conditioned based on the number of times it is invoked . . . . [T]he right to execute can be conditioned on any other parameter so long as it can be measured by the coprocessor to the satisfaction of the source of that right to execute (the software vendor).” (*See, e.g.*, Ex. 1004, Comerford, 2:24-34.) “In order to condition the right to execute . . . there must be: 1) a statement of the condition (or conditions) under which the application software may (or may not) be allowed to execute fully, and 2) some objective criteria against which the condition or conditions can be measured, and 3) a software program which can test the conditions against the criteria and act in a way determined by results of that test.” (*See, e.g.*, *id.* 3:7-17.) “[T]he criteria are stated in software, and more particularly, in the protected or encrypted portion of the application software. As is described in our copending application Ser. No. 927,629, the only form in which application software is available to the user is in encrypted form; because the user does not have access to the decryption key as a data object, he is unable to modify, or even read the protected software. Thus, incorporating the conditions of the right to execute within the protected software results in securing these conditions against alteration by the user or anyone else unless authorized by the software vendor.” (*See, e.g.*, *id.* 3:23-34.) “The criterion tested in the protected software requires that the terminal date be compared to the current date; if the current date is beyond the terminal date, then execution of the protected software does not proceed. . . . It should be apparent to those skilled in the art that another condition which can be substituted for the terminal date condition is the number of times the software is executed. . . . It should be apparent that there are many variations to these specific implementations, including elapsed time, passwords, and combinations of these and other measurables, all of which are within the scope of the invention.” (*See, e.g.*, *id.* 4:14-39.)

	"The flag settings for this particular AK include settings that allow it to be backed up and do not allow it to be moved or erased. . . . . . . An AK installation which proceeded under conditions as described above would allow a person to acquire the right to execute a piece of software for demonstration purposes, typically a one time use. . . . The software vendor is protected from having his code reinstalled repeatedly, using demonstration software, without control." (*See, e.g.*, *id.* 16:43-60.) "The conditions of execution can be stored in the same file as the AK and can be installed at the same time as AK." (*See, e.g.*, *id.* 18:59-61.) [E]ach time the protected application is run on the coprocessor 20, prior to authorizing execution, the application uses the criterion stated in the encrypted application file . . . ." (*See, e.g.*, *id.* 19:4-10.) "Associated with each key are a number of binary flags, a bit for each of the following: Meta, Condition, Erase, Transfer and Backup. It should be understood that this list is a useful subset of such flags and that the set would almost certainly be extended by one skilled in the art." (*See, e.g.*, *id.* 29:25-30.) "One of the multibyte entries is headed 'Condition' and this field includes the data associated with a conditioned key, and thus keys AK3 and AKn include data in that field which can be tested by criteria stored in the application they decrypt to determine if execution is authorized." (*See, e.g.*, *id.* 29:50-55.) (*See, e.g.*, *id.* Figs. 2, 3, 4, 19 (showing showing "conditioned rights-to-execute" and "distribution disk 16").) (*See also* Ex. 1005, '629 application, at 11; Ex. 1001, Grimes Dec., at ¶ 144.)
[24c] limiting each and every access to an unprotected form of the protected data portions in accordance with the rules as enforced by an access mechanism, so that unauthorized access to the protected portions of the data	This limitation is substantially similar to limitation 1d, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1004, Comerford, 2:24-34, 3:7-17, 4:11-39, 16:43-60, 29:25-30, 29:50-55, Figs. 2, 3, 4, 19; Ex. 1005, '629 application, at 9-10, 28-29, 57; *see also* Ex. 1005, '629 application, at 13, 37, 57; Ex. 1006, Chandra, 5:24-30.)

is not to the unprotected form of the protected data portions.	

Claims 25, 30, 32, and 33 are closely related. (Ex. 1001, Grimes Dec., at ¶ 145.) For example, claim 25 recites "[a] device for displaying images" and claim 30 recites "[a] device for outputting images." Comerford discloses both of these limitations because "display 11" is part of the "minimal coprocessor system." (Ex. 1005, '629 application, at 40-41, Fig. 1; Ex. 1001, Grimes Dec., at ¶¶ 145, 147.) Similarly, claim 32 recites "[a] device for outputting an output signal" and claim 33 recites "[a] device for generating an output signal." Comerford discloses both of these limitations because the coprocessor has an "I/O device 154." (Ex. 1001, Grimes Dec., at ¶¶ 149, 151; Ex. 1005, '629 application, at 47, Fig. 1.) Further, the computer system in which the coprocessor is installed is also disclosed as having an "I/O device 19." (Ex. 1001, Grimes Dec., at ¶¶ 149, 151; Ex. 1005, '629 application, at 47, Fig. 1.) All four claims recite "means for storing the rules." Comerford discloses this limitation because it discloses that the coprocessor has volatile and non-volatile memory for storing the right to execute. (Ex. 1005, '629 application, at 15, 36-37, 57; Ex. 1004, Comerford, 3:34-43, 18:56-61, 29:17-20, Figs. 2, 3, 4, 19; Ex. 1001, Grimes Dec., at ¶¶ 145, 147, 149, 151.) The claim charts below demonstrate in detail how Comerford anticipates claims 25, 30, 32, and 33. (Ex. 1001, Grimes Dec., at ¶¶ 145-152.)

25[a]. A device for displaying images	"The software is partitioned into an encrypted portion P_e and an unencrypted (clear text) portion P_c." (*See, e.g.*, Ex. 1005, '629

represented by data comprising protected data portions and rules defining access rights to the data, the device comprising:	application, at 10.) "[I]t is only when the right to use is installed on the suitable coprocessor (which is associated with the host computer on which the user intends to run the software) that the software becomes executable." (*See, e.g.*, *id.* at 9.) (*See, e.g.*, *id.* Fig. 1 (showing "display 11").) "[T]he right to execute might be conditioned by a time period . . . or it could be conditioned based on the number of times it is invoked . . . . [T]he right to execute can be conditioned on any other parameter so long as it can be measured by the coprocessor to the satisfaction of the source of that right to execute (the software vendor)." (*See, e.g.*, Ex. 1004, Comerford, 2:24-34.)
[25b] means for storing the rules;	"In addition to the processor, memory (RAM and ROM) and port address registers (if any) the coprocessor has physically and logically secure memory space which contains ROM and non-volatile memory devices (such as battery backed CMOS RAM or EEPROMs)." (*See, e.g.*, Ex. 1005, '629 application, at 37.) "The non-volatile RAM device is used by the coprocessor as a secure non-volatile memory in which decryption keys AK1, AK2, etc. of initialized applications are stored along with all CSKs." (*See, e.g.*, *id.*) "In order to save (for testing) the conditions which are tested against the programmed criteria, we use some storage space in the non volatile memory of the coprocessor; this storage space has already allocated to it the function of storing the decryption key necessary to decrypt the encrypted software. Thus the storage space allocated to a particular protected piece of software is expanded to include the condition which can be measured against the criteria." (*See, e.g.*, Ex. 1004, Comerford, 3:34-43.) "[T]he coprocessor 20 stores the software decryption key AK in the permanent memory 25. The conditions of execution can be stored in the same file as the AK and can be installed at the same time as AK." (*See, e.g.*, *id.* 18:56-61.) "FIG. 19 is an example of the appearance of a portion of the permanent memory 25 of a typical coprocessor which has been in use for some time and stores a collection of rights to execute." (*See, e.g.*, *id.* 29:17-20.)

	(*See, e.g.*, *id.* Figs. 2, 3, 4, 19 (showing "conditioned rights-to-execute" and "coprocessor 20").) (*See also* Ex. 1005, '629 application, at 15, 36, 42, 57; Ex. 1001, Grimes Dec., at ¶ 146.)
[25c] an access mechanism for accessing the data only in accordance with the rules, whereby user access to an unprotected form of the protected data portions is permitted by the access mechanism only if the rules indicate that the user is allowed to access the protected portions of the data, the access being enforced by the access mechanism; and	This limitation is substantially similar to limitation 1d, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1004, Comerford, 2:24-34, 3:7-17, 4:11-39, 16:43-60, 29:25-30, 29:50-55, Figs. 2, 3, 4, 19; Ex. 1005, '629 application, at 9-10, 28-29, 57; *see also* Ex. 1005, '629 application, at 13, 37, 57; Ex. 1006, Chandra, 5:24-30.)
[25d] means for displaying the images represented by the accessed data.	"The remaining sub-systems, terminal control unit 9, display 11, manual input device 13, disk system control unit 15, disk drive 17 and I/O port 19 can be characterized as having or supporting both addressable elements and mechanical, optical or electro-magnetic (or other) elements which can affect human senses, be affected by human actions, or manipulate a magnetic medium to perform read and write operations involving creating and sensing the boundary between magnetic domains on the magnetic medium." (*See, e.g.*, Ex. 1005, '629 application, at 40.) (*See, e.g.*, *id.* Fig. 1 (showing "display 11").) (*See also id.* at 36, 41; Ex. 1001, Grimes Dec., at ¶ 146.)

30[a]. A device for outputting images represented by data comprising protected data portions and rules defining access rights to the data, the device comprising:	This limitation is substantially similar to limitation 25a, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1005, '629 application, at 9-10, Fig. 1; Ex. 1004, Comerford, 2:24-34.)

[30b] means for storing the rules;	This limitation is substantially similar to limitation 25b, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1004, Comerford, 3:34-43, 18:56-61, 29:17-20, Figs. 2, 3, 4, 19; Ex. 1005, ’629 application, at 37; *see also* Ex. 1005, ’629 application, at 15, 36,42, 57.)
[30c] an access mechanism for accessing the data only in accordance with the rules, whereby user access to an unprotected form of the protected data portions is permitted by the access mechanism only if the rules indicate that the user is allowed to access the protected portions of the data, the access being enforced by the access mechanism; and	This limitation is substantially similar to limitation 25c, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1004, Comerford, 2:24-34, 3:7-17, 4:11-39, 16:43-60, 29:25-30, 29:50-55, Figs. 2, 3, 4, 19; Ex. 1005, ’629 application, at 9-10, 28-29, 57; *see also* Ex. 1005, ’629 application, at 13, 37, 57; Ex. 1006, Chandra, 5:24-30.)
[30d] means for outputting the images represented by the accessed data.	This limitation is substantially similar to limitation 25d, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1005, ’629 application, at 40, Fig. 1; *see also id.* at 36, 41.)

32[a]. A device for outputting an output signal based on data comprising protected data portions and rules defining access rights to the data, the device comprising:	“The software is partitioned into an encrypted portion P_e and an unencrypted (clear text) portion P_c.” (*See, e.g.*, Ex. 1005, ’629 application, at 10.) “[I]t is only when the right to use is installed on the suitable coprocessor (which is associated with the host computer on which the user intends to run the software) that the software becomes executable.” (*See, e.g.*, *id.* at 9.) (*See, e.g.*, *id.* Fig. 1 (showing “I/O ports” 19 and 154).) “[T]he right to execute might be conditioned by a time period . . . or it could be conditioned based on the number of times it is invoked . . . . [T]he right to execute can be conditioned on any other parameter so long as it can be measured by the coprocessor to the satisfaction of the source of that right to execute (the software vendor).” (*See, e.g.*, Ex. 1004, Comerford, 2:24-34.)
[32b] means for storing the	This limitation is substantially similar to limitation 30b, and it

rules;	is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1004, Comerford, 3:34-43, 18:56-61, 29:17-20, Figs. 2, 3, 4, 19; Ex. 1005, ’629 application, at 37; *see also* Ex. 1005, ’629 application, at 15, 36,42, 57.)
[32c] an access mechanism for accessing the data only in accordance with the rules, whereby user access to an unprotected form of the protected data portions is permitted by the access mechanism only if the rules indicate that the user is allowed to access the protected portions of the data, the access being enforced by the access mechanism; and	This limitation is substantially similar to limitation 30c, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1004, Comerford, 2:24-34, 3:7-17, 4:11-39, 16:43-60, 29:25-30, 29:50-55, Figs. 2, 3, 4, 19; Ex. 1005, ’629 application, at 9-10, 28-29, 57; *see also* Ex. 1005, ’629 application, at 13, 37, 57; Ex. 1006, Chandra, 5:24-30.)
[32d] means for outputting the output signal represented by the accessed data.	“If the coprocessor is directly installed . . . in a PC, then it can communicate with the PC through a region of common memory and through a set of registers which reside in the port address space of the PC. . . . The coprocessor controls its bus transceivers and can cause the common memory to be unavailable to the PC for read operations. (This architecture is described in our co-pending [U.S. Pat. No. 4,644,493], filed Sept. 14, 1984.) In the alternative, the coprocessor can communicate with the PC through an I/O port.” (*See, e.g.*, Ex. 1005, ’629 application, at 36-37; *see also* Ex. 1006, Chandra, 15:47.) “The remaining sub-systems, terminal control unit 9, display 11, manual input device 13, disk system control unit 15, disk drive 17 and I/O port 19 can be characterized as having or supporting both addressable elements and mechanical, optical or electro-magnetic (or other) elements which can affect human senses, be affected by human actions, or manipulate a magnetic medium to perform read and write operations involving creating and sensing the boundary between magnetic domains on the magnetic medium.” (*See, e.g.*, Ex. 1005, ’629 application, at 40.)

	"The cartridge 20, storing the transfer token is coupled to the I/O device 154 of the coprocessor (not illustrated) or the I/O device 19 of the PC (as illustrated) via a connector provided for that purpose." (*See, e.g.*, *id.* at 47.) (*See, e.g.*, *id.* Fig. 1 (showing showing "I/O ports" 19 and 154).) (*See also id.* at 41; Ex. 1001, Grimes Dec., at ¶ 150.)

33[a]. A device for generating an output signal corresponding to data comprising protected data portions and rules defining access rights to the digital data, the device comprising:	This limitation is substantially similar to limitation 32a, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1005, '629 application, at 9-10, Fig. 1; Ex. 1004, Comerford, 2:24-34.)
[33b] means for storing the rules;	This limitation is substantially similar to limitation 32b, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1004, Comerford, 3:34-43, 18:56-61, 29:17-20, Figs. 2, 3, 4, 19; Ex. 1005, '629 application, at 37; *see also* Ex. 1005, '629 application, at 15, 36,42, 57.)
[33c] an access mechanism for accessing the digital data only in accordance with the rules, whereby user access to an unprotected form of the protected data portions is permitted by the access mechanism only if the rules indicate that the user is allowed to access the protected portions of the data; and	This limitation is substantially similar to limitation 32c, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1004, Comerford, 2:24-34, 3:7-17, 4:11-39, 16:43-60, 29:25-30, 29:50-55, Figs. 2, 3, 4, 19; Ex. 1005, '629 application, at 9-10, 28-29, 57; *see also* Ex. 1005, '629 application, at 13, 37, 57; Ex. 1006, Chandra, 5:24-30.)
[33d] means for generating the output signal from the accessed data.	This limitation is substantially similar to limitation 32d, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1005, '629 application, at 36-37, 40, 47, Fig. 1; *see also id.* at 41; Ex. 1006, Chandra, 15:47.)

The limitations of claim 36 are similar to those in previous claims, but claim 36 recites "[a] process control system," while the previously addressed claims recited methods and devices. (Ex. 1001, Grimes Dec., at ¶ 153.) All of the limitations of claim 38 are substantially similar to the limitations of claim 36, as the only difference is that claim 38 recites “[a] general purpose computer system” instead of “[a] process control system.” (*Id.* at ¶ 155.) The claim charts below demonstrates in detail how Comerford anticipates claims 36 and 38. (Ex. 1001, Grimes Dec., at ¶¶ 153-156.)

36[a]. A process control system comprising a device for controlling access to data,	“The encrypted portion, P_e, of the software will be decrypted and executed by a physically and logically secure coprocessor if the coprocessor possesses the decryption key which embodies the right to execute. The protected part of the software is, thus, never exposed in plaintext form and never executed by unauthorized systems.” (*See, e.g.*, Ex. 1005, ’629 application, at 10.) “The logical and physical security of the coprocessor memory prevents the user from having access to plaintext or executable form of the protected software.” (*See, e.g.*, *id.* at 16.)
[36b] the data comprising protected data portions and rules defining access rights to the data,	“The software is partitioned into an encrypted portion P_e and an unencrypted (clear text) portion P_c.” (*See, e.g.*, *id.* at 10.) “As shown in Fig. 3 the three files may be distributed as unit . . . . A first file is an encrypted software decryption key EAK. The second file is the software which includes both plain text software (PART 1) and protected or encrypted software (PART 2) (EAK (Software, Part 2)).” (*See, e.g.*, *id.* at 45.) “[T]he right to execute might be conditioned by a time period . . . or it could be conditioned based on the number of times it is invoked . . . . [T]he right to execute can be conditioned on any other parameter so long as it can be measured by the coprocessor to the satisfaction of the source of that right to execute (the software vendor).” (*See, e.g.*, Ex. 1004, Comerford, 2:24-34.) “In order to condition the right to execute . . . there must be: 1) a statement of the condition (or conditions) under which the application software may (or may not) be allowed to execute fully, and 2) some objective criteria against which the condition or

	conditions can be measured, and 3) a software program which can test the conditions against the criteria and act in a way determined by results of that test." (*See, e.g.*, *id.* 3:7-17.) "[T]he criteria are stated in software, and more particularly, in the protected or encrypted portion of the application software. As is described in our copending application Ser. No. 927,629, the only form in which application software is available to the user is in encrypted form; because the user does not have access to the decryption key as a data object, he is unable to modify, or even read the protected software. Thus, incorporating the conditions of the right to execute within the protected software results in securing these conditions against alteration by the user or anyone else unless authorized by the software vendor." (*See, e.g.*, *id.* 3:23-34.) "The criterion tested in the protected software requires that the terminal date be compared to the current date; if the current date is beyond the terminal date, then execution of the protected software does not proceed. . . . It should be apparent to those skilled in the art that another condition which can be substituted for the terminal date condition is the number of times the software is executed. . . . It should be apparent that there are many variations to these specific implementations, including elapsed time, passwords, and combinations of these and other measurables, all of which are within the scope of the invention." (*See, e.g.*, *id.* 4:14-39.) "The flag settings for this particular AK include settings that allow it to be backed up and do not allow it to be moved or erased. . . . . . . An AK installation which proceeded under conditions as described above would allow a person to acquire the right to execute a piece of software for demonstration purposes, typically a one time use. . . . The software vendor is protected from having his code reinstalled repeatedly, using demonstration software, without control." (*See, e.g.*, *id.* 16:43-60.) "The conditions of execution can be stored in the same file as the AK and can be installed at the same time as AK." (*See, e.g.*, *id.* 18:59-61.) [E]ach time the protected application is run on the coprocessor

	20, prior to authorizing execution, the application uses the criterion stated in the encrypted application file . . . .” (*See, e.g.*, *id.* 19:4-10.) “Associated with each key are a number of binary flags, a bit for each of the following: Meta, Condition, Erase, Transfer and Backup. It should be understood that this list is a useful subset of such flags and that the set would almost certainly be extended by one skilled in the art.” (*See, e.g.*, *id.* 29:25-30.) “One of the multibyte entries is headed ‘Condition’ and this field includes the data associated with a conditioned key, and thus keys AK3 and AKn include data in that field which can be tested by criteria stored in the application they decrypt to determine if execution is authorized.” (*See, e.g.*, *id.* 29:50-55.) (*See, e.g.*, *id.* Figs. 2, 3, 4, 19 (showing “conditioned rights-to-execute” and “distribution disk 16”).)
[36c] the device comprising: means for storing the rules; and	This limitation is substantially similar to limitation 25b, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1004, Comerford, 3:34-43, 18:56-61, 29:17-20, Figs. 2, 3, 4, 19; Ex. 1005, ’629 application, at 37; *see also* Ex. 1005, ’629 application, at 15, 36,42, 57.)
[36d] an access mechanism for accessing the unprotected form of the protected data portions only in accordance with the rules, whereby output of an unprotected form of the protected data portions is permitted by the access mechanism only in such manner as is permitted by the rules.	This limitation is substantially similar to limitation 1d, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1004, Comerford, 2:24-34, 3:7-17, 4:11-39, 16:43-60, 29:25-30, 29:50-55, Figs. 2, 3, 4, 19; Ex. 1005, ’629 application, at 9-10, 28-29, 57; *see also* Ex. 1005, ’629 application, at 13, 37, 57; Ex. 1006, Chandra, 5:24-30.)

38[a]. A general purpose computer system comprising a device for controlling access to data,	This limitation is substantially similar to limitation 36a, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex.

	1005, ’629 application, at 10, 16.)
[38b] the data comprising protected data portions and rules defining access rights to the data,	This limitation is substantially similar to limitation 36b, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1004, Comerford, 2:24-34, 3:7-17, 3:23-34, 4:14-39, 16:43-60, 18:59-61, 19:4-10, 29:25-30, 29:50-55, Figs. 2, 3, 4, 19; Ex. 1005, ’629 application, at 10, 45.)
[38c] the device comprising: storage means for storing the rules; and	This limitation is substantially similar to limitation 36c, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1004, Comerford, 3:34-43, 18:56-61, 29:17-20, Figs. 2, 3, 4, 19; Ex. 1005, ’629 application, at 37; *see also* Ex. 1005, ’629 application, at 15, 36,42, 57.)
[38d] an access mechanism for accessing the unprotected form of the protected data portions only in accordance with the rules, whereby user access to an unprotected form of the protected data portions is permitted by the access mechanism only if the rules indicate that the user is allowed to access the protected portions of the data.	This limitation is substantially similar to limitation 36d, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1004, Comerford, 2:24-34, 3:7-17, 4:11-39, 16:43-60, 29:25-30, 29:50-55, Figs. 2, 3, 4, 19; Ex. 1005, ’629 application, at 9-10, 28-29, 57; *see also* Ex. 1005, ’629 application, at 13, 37, 57; Ex. 1006, Chandra, 5:24-30.)

C. Comerford in View of Abraham Renders Claims 14-20, 26-27, 29, 37, and 39 Obvious

Claims 14-20, 26-27, 29, 37, and 39 all recite (or depend from clams that recite) the limitation of “at least one internal rule built in the access mechanism.” The ’409 patent discloses “plac[ing] a global set of rules (a global permission list) in the [access] mechanism,” which allows a user to “thereby customize a particular access mechanism.” (*See* Ex. 1002, ’409 patent, 32:30-53, 34:29-43.) Abraham discloses this limitation in the form of “command configuration data,” which “defines the authorization required by [a] device to execute a requested command in that device.” (Ex. 1001, Grimes Dec., at ¶ 157; *see, e.g.*, Ex. 1007, Abraham, 2:17-22.) Like what is disclosed in the ’409 patent, “[t]here is a unique set of command configuration data for each of the system security devices in the system.” (Ex. 1001, Grimes Dec., at ¶ 157; Ex. 1007, Abraham, 9:37-39.) The remaining limitations of claims 14-20, 26-27, 29, 37, and 39 are disclosed by Comerford, as detailed above and below, and thus, Comerford in view of Abraham renders claims 14-20, 26-27, 29, 37, and 39 obvious. (Ex. 1001, Grimes Dec., at ¶ 157.)

Abraham discloses “a highly flexible and secure identification IC card and a distributed authorization system.” (Ex. 1007, Abraham, 1:59-61.) User authorizations are embodied “in the form of several independent profiles.” (*Id.* 2:1-4.) “Access to a command is controlled by the content of a user’s authorization profile in conjunction with the command configuration data for the requested command.” (*Id.* 2:7-10.) “The user profiles may be downloaded into other security devices in the system for the purpose of controlling use of commands, files, and programs in system component devices, in addition to the IC card itself,” but “[t]he device command configuration data is not downloaded.” (*Id.* 2:11-14, 2:17-18.) “[T]he device command configuration data defines the authorization required by that device to execute a requested command in that device.” (*Id.* 2:18-22.)

At the time of invention, it would have been obvious to one of ordinary skill in the art to combine Comerford and Abraham. (Ex. 1001, Grimes Dec., at ¶ 159.) First, Comerford and Abraham are analogous art because they are within the field of endeavor of the ’409 patent (control of distribution and access of digital property) and are pertinent to the same purpose or goal (controlling the access to protected data) as the ’409 patent’s claimed inventions. (*Id.*) Both patents relate to the protection of distributed digital data, and both disclose inventions that protect such data by protecting portions of the digital data using encryption. (*Id.*)

At the time of invention, one of ordinary skill in the art would have recognized Comerford as one solution that enables software vendors to distribute their software with confidence that only authorized users will have the ability to execute the software on their coprocessors and knowing that the coprocessors will enforce any conditions of execution. (*Id.* at ¶ 160.) Such a person, however, would also have recognized other problems that would have led him to combine Comerford and Abraham. (*Id.*) For example, at the time of invention, such a person would have recognized a need to limit the access allowed by certain devices regardless of the person using the device. (*Id.*) One of ordinary skill in the art would have known that data owners and distributors might wish to apply different levels of access to devices located in secured facilities as opposed to devices located in public places. (*Id.*) Further, one of ordinary skill in the art would have known that data owners and distributors might wish to apply different levels of access to devices located in different countries. (*Id.*) Also, specific devices might have different capabilities than other devices that might lead to a desire by data owners and distributors to apply different levels of access based on the specific capabilities of the relevant devices. (*Id.*) In seeking to address these problems, at the time of invention, it would have been obvious to one of ordinary skill in the art to supplement Comerford's teaching of a conditioned right to execute with Abraham's teaching of command configuration data that defines the authorization required by particular devices. (*Id.*) At the time of invention, one of ordinary skill in the art would have viewed such a combination as the use of a known technique to improve a known device in a manner that would yield a predictable result. (*Id.*) The combination of Comerford and Abraham discloses all of the limitations of claims 14-20, 26-27, 29, 37, and 39 and renders these claims obvious. (*Id.*)

Claim 14 depends from claim 1 and further recites: "wherein the rules defining access rights include at least one internal rule built in the access mechanism." As explained above, Abraham discloses an "internal rule built in the access mechanism" in the form of "command configuration data," which "defines the authorization required by [a] device to execute a requested command in that device." (*Id.* at ¶ 161; *see, e.g.*, Ex. 1007, Abraham, 2:17-22.) The additional disclosures in the claim chart below demonstrate in detail how Comerford in view of Abraham renders claim 14 obvious. (Ex. 1001, Grimes Dec., at ¶ 162.)

14. A method as in claim 1 wherein the rules defining access rights include at least one internal rule built in the	Comerford discloses claim 1 as detailed above. "The device command configuration data is not downloaded. . . . [T]he device command configuration data defines the authorization required by that device to execute a requested command in that device. The same or different commands in other devices to which the user's authorization profile is transferred may have greater or lesser security requirements defined in, their command configurations." (*See, e.g.*, Ex.

access mechanism.	1007, Abraham, 2:17-26.) "The command configuration data 181 is independent of the user authorization profile, but consists of a number of prerequisite conditions and authorizations for each command. There is a unique set of command configuration data for each of the system security devices in the system." (*See, e.g.*, *id.* 9:34-39.) (*See also id.* 15:53-16:6; Ex. 1001, Grimes Dec., at ¶ 162.)

Claim 15 depends from claim 14 and further recites: "wherein the at least one internal rule cannot be made less restrictive by any other rules." As detailed above, Abraham discloses "command configuration data," which "defines the authorization required by [a] device to execute a requested command in that device." (Ex. 1007, Abraham, 2:17-22.) This "command configuration data" "cannot be made less restrictive by any other rules," as it "consists of a number of ***prerequisite*** conditions and authorizations for each command." (*See, e.g.*, *id.* 8:52-63, 9:34-37 (emphasis added); Ex. 1001, Grimes Dec., at ¶ 163.) Accordingly, Comerford in view of Abraham renders claim 15 obvious as detailed in the claim chart below. (Ex. 1001, Grimes Dec., at ¶¶ 163-164.)

15. A method as in claim 14 wherein the at least one internal rule cannot be made less restrictive by any other rules.	"A user's authority is defined by the contents of a related user profile in the table of user profiles 179. The requirements for execution of the selected command are defined in command configuration data table 181 by the execution prerequisites for that command. These two items of information from the tables are examined to determine if the user is permitted to execute the command. These steps are set out in more detail in FIG. 9." (*See, e.g.*, Ex. 1007, Abraham, 8:56-63.) "The command configuration data 181 is independent of the user authorization profile, but consists of a number of prerequisite conditions and authorizations for each command." (*See, e.g.*, *id.* 9:34-37.)

Claim also 16 depends from claim 14 and further recites: "wherein the access mechanism is contained in a stand-alone device." Comerford, itself, discloses an access mechanism contained in a stand-alone device in the form of a "computer which is associated with a specified, physically secure coprocessor." (Ex. 1001, Grimes Dec., at ¶ 165; Ex. 1005, '629 application, at 4, Figs. 1, 5.) The additional disclosures in the claim chart below demonstrate in detail how Comerford in view of Abraham renders claim 16 obvious. (Ex. 1001, Grimes Dec., at ¶ 166.)

16. A method as in claim 14 wherein the access mechanism is contained in a stand-alone device.	"In particular a mechanism is provided which restricts software, distributed on magnetic disk or other medium, to use on any computer which is associated with a specified, physically secure coprocessor . . . ." (*See, e.g.*, Ex. 1005, '629 application, at 4.) (*See, e.g.*, *id.* Fig. 1 (showing the "coprocessor"), Fig. 5 (showing the "composite computing system").)

Claim 17 depends from claim 16 and further recites: "wherein the stand-alone device is selected from the group consisting of: a facsimile machine, a television, a VCR, a laser printer, a telephone, a laser disk player, and a computer system." Comerford discloses a "computer which is associated with a specified, physically secure coprocessor," which constitutes "a computer system." (Ex. 1001, Grimes Dec., at ¶ 167; *see, e.g.*, Ex. 1005, '629 application, at 4, Figs. 1, 5.) Accordingly, Comerford in view of Abraham renders claim 17 obvious as detailed in the claim chart below. (Ex. 1001, Grimes Dec., at ¶¶ 167-168.)

17. A method as in claim 16 wherein the stand-alone device is selected from the group consisting of: a facsimile machine, a	"[A] mechanism is provided which restricts software . . . to use on any computer which is associated with a specified, physically secure coprocessor . . . ." (*See, e.g.*, Ex. 1005, '629

television, a VCR, a laser printer, a telephone, a laser disk player, and a computer system.	application, at 4.) (*See, e.g.*, *id.* Figs. 1, 5 (showing the "coprocessor" and "composite computing system").)

Claim 18 depends from claim 1 and further recites: "wherein the at least one internal rule comprises access control rights to the data." Abraham's disclosure of "command configuration data[, which] defines the authorization required by that device to execute a requested command in that device," satisfies this limitation. (Ex. 1001, Grimes Dec., at ¶ 169; Ex. 1007, Abraham, 2:18-22.) The additional disclosures in the claim chart below demonstrate in detail how Comerford in view of Abraham renders claim 18 obvious. (Ex. 1001, Grimes Dec., at ¶¶ 169-170.)

18[a]. A method as in claim 1, wherein the access mechanism is contained in a stand-alone device selected from the group comprising: a facsimile machine, a television, a VCR, a laser printer, a telephone, a laser disk player, and a computer system; and	Comerford discloses claim 1 as detailed above. This limitation is substantially similar to claim 17, and it is disclosed by the same portions of Comerford detailed in full for that claim above. (*See, e.g.*, Ex. 1005, '629 application, at 4, Figs. 1, 5.)
[18b]wherein the rules defining access rights include at least one internal rule built-in to the access mechanism; and	This limitation is substantially similar to claim 14, and it is disclosed by the same portions of Abraham detailed in full for that claim above. (*See, e.g.,* Ex. 1007, Abraham, 2:17-26, 9:34-39; *see also id.* 15:53-16:6.)
[18c] wherein the at least one internal rule comprises access control rights to the data.	"[T]he device command configuration data defines the authorization required by that device to execute a requested command in that device. The same or different commands in other devices to which the user's authorization profile is transferred may have greater or lesser security requirements defined in, their command configurations." (*See, e.g.*, *id.* 2:18-26.) "The command configuration data 181 is independent of the user authorization profile, but consists of a number of

	prerequisite conditions and authorizations for each command." (*See, e.g.*, *id.* 9:34-37.)

Claim 19 also depends from claim 1 and further recites: "providing a distribution rule." Comerford, itself, discloses that the only users that can decrypt and execute the protected software are those users who satisfy the specified conditions of a conditioned right to execute. (Ex. 1001, Grimes Dec., at ¶ 171; Ex. 1004, Comerford, 4:11-39.) Additionally, Comerford discloses a demonstration-software embodiment in which flag settings are used by the software vendor to "protect[] from having his code reinstalled repeatedly . . . without control," which discloses this limitation. (Ex. 1001, Grimes Dec., at ¶ 171; Ex. 1004, Comerford, 16:33-60.) Claim 19 further recites "wherein the rules defining access rights comprise the distribution rule and at least one internal rule built in to the access mechanism." The disclosure for claim limitation 19a—"providing a distribution rule"—is also applicable to this second limitation, so only pinpoint citations for this disclosure is provided for this limitation in the claim chart below. The additional disclosures in the claim chart below demonstrate in detail how Comerford in view of Abraham renders claim 19 obvious. (Ex. 1001, Grimes Dec., at ¶¶ 171-172.)

19[a]. A method as in claim 1, further comprising: providing a distribution rule,	Comerford discloses claim 1 as detailed above. "[I]t is only when the right to use is installed on the suitable coprocessor (which is associated with the host computer on which the user intends to run the software) that the software becomes executable." (*See, e.g.*, Ex. 1005, '629 application, at 9.) "In order to be effective, and decrypt the encrypted portion of

	the protected software, the coprocessor must be provided with the decryption key (Right-to-Execute or RTE, also referred to as AK or Application Key) needed to render the encrypted portion of software executable." (*See, e.g.*, *id.* at 10.) "The user is also provided with a physically and logically secure coprocessor. The physically and logically secure coprocessor has in permanent memory the hardware vendor's decryption key(s) CSK1, CSK2, etc." (*See, e.g.*, *id.* at 14.) "On the first running of the software the encrypted software key EAK is transferred to the coprocessor and is decrypted by the coprocessor using the required CSK to obtain AK." (*See, e.g.*, *id.* at 15.) "[I]t is the encrypted fraction of the software which will be protected from redistribution by the user." (*See, e.g.*, *id.* at 33.) "In order to condition the right to execute . . . there must be: 1) a statement of the condition (or conditions) under which the application software may (or may not) be allowed to execute fully, and 2) some objective criteria against which the condition or conditions can be measured, and 3) a software program which can test the conditions against the criteria and act in a way determined by results of that test." (*See, e.g.*, Ex. 1004, Comerford, 3:7-17.) "The criterion tested in the protected software requires that the terminal date be compared to the current date; if the current date is beyond the terminal date, then execution of the protected software does not proceed. . . . It should be apparent to those skilled in the art that another condition which can be substituted for the terminal date condition is the number of times the software is executed. . . . It should be apparent that there are many variations to these specific implementations, including elapsed time, passwords, and combinations of these and other measurables, all of which are within the scope of the invention." (*See, e.g.*, *id.* 4:14-39.) "The flag settings for this particular AK include settings that allow it to be backed up and do not allow it to be moved or erased. . . . An AK installation which proceeded under

	conditions as described above would allow a person to acquire the right to execute a piece of software for demonstration purposes, typically a one time use. . . . The software vendor is protected from having his code reinstalled repeatedly, using demonstration software, without control." (*See, e.g.*, *id.* 16:43-60.) "Associated with each key are a number of binary flags, a bit for each of the following: Meta, Condition, Erase, Transfer and Backup. It should be understood that this list is a useful subset of such flags and that the set would almost certainly be extended by one skilled in the art." (*See, e.g.*, *id.* 29:25-30.) (*See also* Ex. 1005, '629 application, at 17; Ex. 1001, Grimes Dec., at ¶ 172.)
[19b] wherein the rules defining access rights comprise the distribution rule and at least one internal rule built in to the access mechanism.	A portion of this limitation is substantially similar to limitation 19a, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1004, Comerford, 3:7-17, 4:14-39, 16:43-60, 29:25-30; Ex. 1005, '629 application, at 9-10, 14-15, 33; *see also* Ex. 1005, '629 application, at 17.) A portion of this limitation is substantially similar to claim 14, and it is disclosed by the same portions of Abraham detailed in full for that claim above. (*See, e.g.*, Ex. 1007, Abraham, 2:17-26, 9:34-39; *see also id.* 15:53-16:6.)

Claim 20 depends from claim 19 and further recites: "wherein the distribution rule comprises a data decrypting key." Comerford, itself, discloses that "[i]n order to be effective, and decrypt the encrypted portion of the protected software, the coprocessor must be provided with the decryption key (Right-to-Execute or RTE, also referred to as AK or Application Key) needed to render the encrypted portion of software executable," which satisfies this limitation. (Ex. 1001, Grimes Dec., at ¶ 173; Ex. 1005, '629 application, at 9.)

The additional disclosures in the claim chart below demonstrate in detail how Comerford in view of Abraham renders claim 20 obvious. (Ex. 1001, Grimes Dec., at ¶¶ 173-174.)

20[a]. A method as in claim 19 wherein the protecting of portions of the data comprises encrypting the portions of the data using a data encrypting key having a corresponding data decrypting key, and	This limitation is substantially similar to limitation 3a, and it is disclosed by the same portions of Comerford detailed in full for that limitation above. (*See, e.g.*, Ex. 1005, ’629 application, at 33-34, 55, 57.)
[20b] wherein the distribution rule comprises a data decrypting key.	“In order to be effective, and decrypt the encrypted portion of the protected software, the coprocessor must be provided with the decryption key (Right-to-Execute or RTE, also referred to as AK or Application Key) needed to render the encrypted portion of software executable.” (*See, e.g.*, *id.* at 10.) “The user is also provided with a physically and logically secure coprocessor. The physically and logically secure coprocessor has in permanent memory the hardware vendor’s decryption key(s) CSK1, CSK2, etc.” (*See, e.g.*, *id.* at 14.) “On the first running of the software the encrypted software key EAK is transferred to the coprocessor and is decrypted by the coprocessor using the required CSK to obtain AK.” (*See, e.g.*, *id.* at 15.) (*See also id.* at 17; Ex. 1001, Grimes Dec., at ¶ 174.)

Claim 26 depends from claim 25 and further recites: “wherein the rules defining access rights include at least one internal rule built in the access mechanism.” The additional disclosures in the claim chart below demonstrate in detail how Comerford in view of Abraham renders claim 26 obvious. (Ex. 1001, Grimes Dec., at ¶¶ 175-176.)

26. A device as in claim 25 wherein the rules defining access rights	Comerford discloses claim 25 as detailed above.

include at least one internal rule built in the access mechanism.	This limitation is substantially similar to claim 14, and it is disclosed by the same portions of Abraham detailed in full for that claim above. (*See, e.g.*, Ex. 1007, Abraham, 2:17-26, 9:34-39; *see also id.* 15:53-16:6.)

Claim 27 depends from claim 26 and further recites: "wherein the internal rules cannot be made less restrictive by any other rules." Abraham discloses "command configuration data" that "cannot be made less restrictive by any other rules," as it "consists of a number of ***prerequisite*** conditions and authorizations for each command." (Ex. 1001, Grimes Dec., at ¶ 177; *see, e.g.*, Ex. 1007, Abraham, 8:52-63, 9:34-37 (emphasis added).) Accordingly, Comerford in view of Abraham renders claim 27 obvious as detailed in the claim chart below. (Ex. 1001, Grimes Dec., at ¶¶ 177-178.)

27. A device as in claim 26 wherein the internal rules cannot be made less restrictive by any other rules	This limitation is substantially similar to claim 15, and it is disclosed by the same portions of Abraham detailed in full for that claim above. (*See, e.g.*, Ex. 1007, Abraham, 8:56-63, 9:34-37.)

Claim 29 depends from claim 26 and further recites: "wherein the device is selected from the group consisting of: a VCR, a laser disk player, and a computer system." Comerford, itself, discloses a "computer which is associated with a specified, physically secure coprocessor," which constitutes "a computer system." (Ex. 1001, Grimes Dec., at ¶ 179; *see, e.g.*, Ex. 1005, '629 application, at 4, Figs. 1, 5.) Accordingly, Comerford in view of Abraham renders claim 29 obvious as detailed in the claim chart below. (Ex. 1001, Grimes Dec., at ¶¶ 179-180.)

29. A device as in claim 26 wherein the device is selected from the group consisting of: a VCR, a laser disk player, and a computer system.	"[A] mechanism is provided which restricts software . . . to use on any computer which is associated with a specified, physically secure coprocessor . . . ." (*See, e.g.*, Ex. 1005, '629 application, at 4.) (*See, e.g.*, *id.* Figs. 1, 5 (showing the "coprocessor" and "composite computing system").)

Claims 37 and 39 depend from claims disclosed by Comerford, as detailed above, add they additionally recite: "wherein the rules defining access rights include at least one internal rule built in the access mechanism." As explained above, Abraham discloses this limitation, as detailed in the claim charts below, which demonstrate in detail how Comerford in view of Abraham renders claims 37 and 39 obvious. (Ex. 1001, Grimes Dec., at ¶¶ 181-184.)

37. A process control system as in claim 36 wherein the rules defining access rights include at least one internal rule built in the access mechanism.	Comerford discloses claim 36 as detailed above. This limitation is substantially similar to claim 14, and it is disclosed by the same portions of Abraham detailed in full for that claim above. (*See, e.g.*, Ex. 1007, Abraham, 2:17-26, 9:34-39; *see also id.* 15:53-16:6.)

39. A computer system as in claim 38 wherein the rules defining access rights include at least one internal rule built in the access mechanism.	Comerford discloses claim 38 as detailed above. This limitation is substantially similar to claim 14, and it is disclosed by the same portions of Abraham detailed in full for that claim above. (*See, e.g.*, Ex. 1007, Abraham, 2:17-26, 9:34-39; *see also id.* 15:53-16:6.)

VII. CONCLUSION

For at least the reasons set forth above, there is a reasonable likelihood of success as to Petitioners' claim that claims 1-11, 13-21, 23-27, 29-30, 32-33, and 36-39 of the '409 patent are not patent eligible. Accordingly, Petitioners respectfully request institution of IPR for claims 1-11, 13-21, 23-27, 29-30, 32-33, and 36-39 of the '409 patent for each of grounds presented herein.

Respectfully submitted,

Dated: May 1, 2014

/Joseph Melnik/
Joseph Melnik
Reg. No. 48,741
Jones Day
1755 Embarcadero Road
Palo Alto, CA 94303
Lead Counsel for Petitioners

LEAD COUNSEL	BACK-UP COUNSEL
Joseph Melnik (Reg. No. 48,741) (jmelnik@jonesday.com) Jones Day 1755 Embarcadero Road Palo Alto, CA 94303 T: (650) 739-3939; F: (650) 739-3900	Geoffrey K. Gavin (Reg. No. 47,591) (ggavin@jonesday.com) Jones Day 1420 Peachtree Street, N.E., Suite 800 Atlanta, GA 30309-3053 T: (404) 521-3939; F: (404) 581-8330
BACK-UP COUNSEL	BACK-UP COUNSEL
Marc Vander Tuig (Reg. No. 57,964) (mvandertuig@senniger.com) Senniger Powers LLP 100 North Broadway, 17th Floor St. Louis, MO 63102 T: (314) 345-7019; F: (314) 345-7600	Jason S. Jackson (Reg. No. 56,733) (jason.jackson@kutakrock.com) Kutak Rock LLP 1650 Farnam St., The Omaha Building Omaha, Nebraska 68102 T: (402) 231-8359; F: (402) 346-1148

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105, the undersigned certifies that on May 1, 2014, a complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits were provided via Express Mail, costs prepaid, to the Patent Owner by serving the correspondence address of record as follows:

Perkins Coie LLP – SEA General
Patent-SEA
P.O. Box 1247
Seattle, WA 98111-1247

A complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits were also provided via UPS overnight delivery, costs prepaid, to the Patent Owner's litigation counsel, as follows, whom Petitioners know as likely to effect service:

Ms. Elizabeth Day
FEINBERG DAY ALBERTI & THOMPSON LLP
1600 El Camino Real, Suite 280
Menlo Park, CA 94025

Dated: May 1, 2014

/Joseph Melnik/
Joseph Melnik
Reg. No. 48,741
Jones Day
1755 Embarcadero Road
Palo Alto, CA 94303
Lead Counsel for Petitioners