Trials@uspto.gov
571-272-7822

Paper 12
Entered: September 22, 2014

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

INTERNATIONAL BUSINESS MACHINES CORPORATION,
Petitioner,

v.

INTELLECTUAL VENTURES II LLC,
Patent Owner.

Case IPR2014-00672
Patent 6,314,409 B2

Before KRISTEN L. DROESCH, JENNIFER S. BISK, and JUSTIN BUSCH, *Administrative Patent Judges.*

DROESCH, *Administrative Patent Judge.*

DECISION
Denying Institution of *Inter Partes* Review
37 C.F.R. § 42.108

I. INTRODUCTION

A. Background

International Business Machines Corporation ("Petitioner") filed a Petition[1] (Paper 4, "Petition" or "Pet.") to institute an *inter partes* review of claims 1–11 and 13–21 ("the challenged claims") of U.S. Patent No. 6,314,409 B2 (Ex. 1006, "the '409 Patent"). 35 U.S.C. §§ 311–319. Intellectual Ventures II LLC ("Patent Owner") timely filed a Preliminary Response to the Petition. Paper 9 ("Prelim. Resp."). We determine on this record that, under 35 U.S.C. § 314(a), the Petition does not demonstrate a reasonable likelihood that Petitioner would prevail in showing that claims 1–11 and 13–21 are unpatentable.

B. Related Proceedings

Petitioner indicates the '409 Patent is at issue in several district court proceedings involving numerous parties. Pet. 2, Paper 11 ("Second Amended Mandatory Notice") 2–3. Petitioner further indicates that none of the district court proceedings name Petitioner as a defendant. Pet. 2; Second Amended Mandatory Notice 2.

Petitioner concurrently filed a petition for *inter partes* review of claims 23–27, 29–30, 32–33, and 36–40 of the '409 Patent (IPR2014-00673). Second Amended Mandatory Notice 3. Compass Bank, Commerce Bancshares, Inc., and First National Bank of Omaha collectively filed two petitions for *inter partes* review of the '409 Patent (IPR2014-00719, IPR2014-00722). *Id.* J.P. Morgan Chase & Co., JPMorgan Chase Bank, Nat'l Ass'n, Chase Bank USA, Nat'l Ass'n, Chase Paymentech Solutions

[1] "Petition" and "Pet." refer to the Corrected Petition filed April 28, 2014.

LLC, and Paymentech LLC collectively filed a petition for covered business method review of the '409 Patent (CBM2014-00157). *Id.* at 4.

C. The '409 Patent (Ex. 1006)

The '409 Patent relates to methods, devices, and systems for controlling access to, and use, distribution, and secondary distribution of data. Ex. 1006, Abs.; col. 6, l. 63–col. 7, l. 9.

Figure 1 of the '409 Patent is reproduced below:

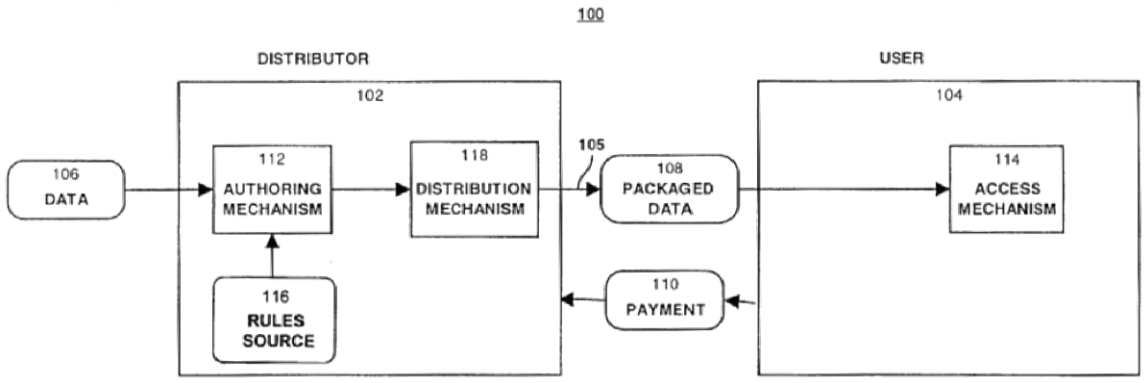

Figure 1 depicts digital data access and distribution system 100, including distributor 102 and user 104. Ex. 1006, col. 9, ll. 11–13, 51–55. Distributor 102 provides packaged data 108 over communication channel 105 to user 104 in return for payment 110. *Id*. at col. 9, ll. 55–58. Specifically, authoring mechanism 112 of distributor 102 produces packaged data 108 from data 106, and distribution mechanism 118 of distributor 102 provides packaged data 108 to user 104. *Id.* at col. 9, ll. 61–64. Packaged data 108 includes an encrypted body part, an unencrypted body part, and access rules 116 in encrypted form. *Id*. at col. 9, ll. 64–66; col. 10, ll. 47–53, 60–65; *see id.* at Fig. 2. Packaged data 108 can be transmitted openly using communication channel 105, which may be insecure. *Id*. at col. 15, ll. 25–29; col. 24, ll. 49–51. Access mechanism 114 enables user 104 to access

packaged data 108 in controlled ways depending on access rules 116. *Id*. at col. 10, ll. 1–5; col. 15, ll. 31–35; col. 17, ll. 45–52. Transmission, printing, display, and output of an unencrypted copy of the data by user 104 also can be prevented or restricted according to access rules. *Id.* at col. 15, ll. 50–54; col. 17, ll. 24–40; col. 25, ll. 15–28; col. 25, l. 59–col. 26, l. 6; col. 26, ll. 11–29; col. 27, ll. 11–24.

A user may invoke access mechanism 114 by accessing an object (data) via an insecure operating system which invokes access mechanism 114. Ex. 1006, col. 17, l. 67–col. 18, l. 7; col. 18, ll. 18–21.

Figure 10a of the ’409 Patent is reproduced below:

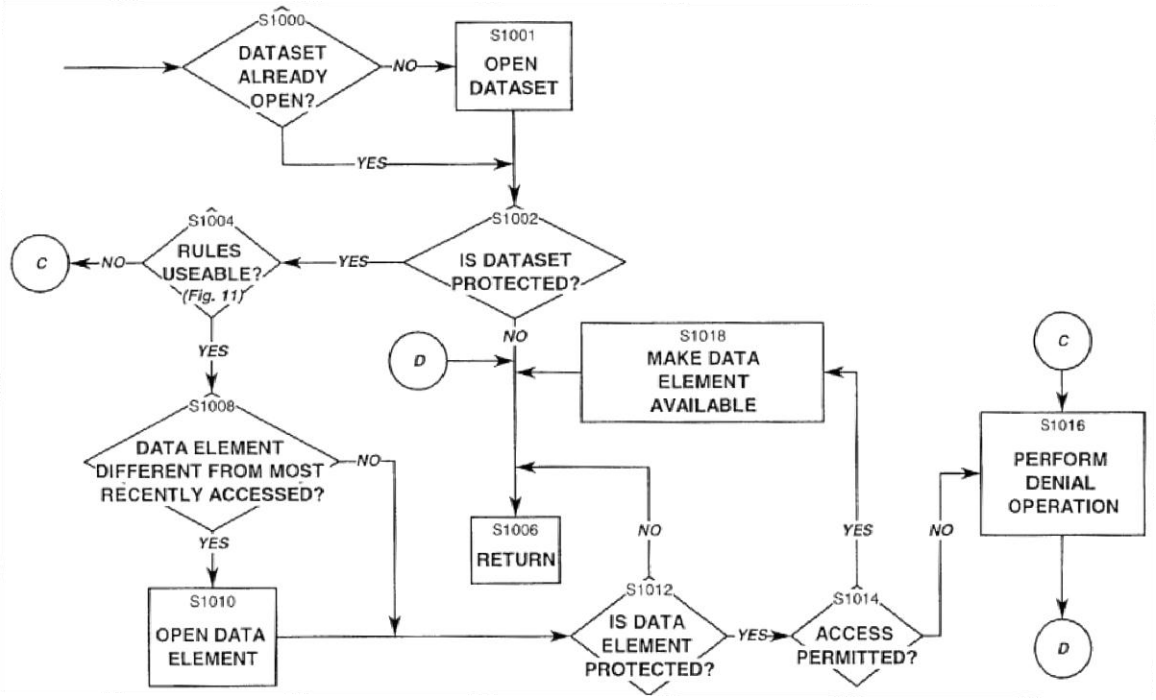

Figure 10a depicts a flow chart of data access using access mechanism 114. Ex. 1006, col. 9, ll. 30–31. Access mechanism 114 first determines whether the data set containing the data elements is already open (step S1000). *Id.* at col. 18, ll. 22–24. If the data set is not already open, access mechanism 114

opens the data set (step S1001). *Id.* at col. 18, ll. 24–25. Next, access mechanism 114 determines whether the dataset is protected (step S1002), and, if it is protected, determines whether the rules for the dataset are usable (step S1004). *Id.* at col. 18, ll. 25–27, 33–38. If the rules are usable (step S1004), access mechanism 114 determines whether the data element being accessed is different from the most recently accessed data element (step S1008), and opens the data element (step S1010) if it is different. *Id.* at col. 18, ll. 39–43. Next, access mechanism 114 determines whether the data element is protected (step S1012) and whether access is permitted according to the rules (step S1014), and makes the data element available (step S1018) if access to the data element is permitted. *Id.* at col. 18, ll. 44–59. Following these determinations, control returns to the invoking process (step S1006). *Id.*

D. Illustrative Claims

Claims 1 and 21 are independent claims. Claims 2–11 and 13–20 depend from claim 1. Claims 1 and 21 are illustrative:

> 1. A method of distributing data, the method comprising:
> protecting portions of the data; and
> openly distributing the protected portions of the data, 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 unauthorized access to the protected portions of the data is not to the unprotected form of the protected portions of the data.
>
> 21. A method of distributing data for subsequent controlled use of the data by a user, the method comprising:
> protecting portions of the data;

protecting rules defining access rights to the data; and
openly distributing the protected portions of the data and the protected rules, whereby
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.

II. ANALYSIS

A. Claim Construction

In an *inter partes* review, claim terms are given their broadest reasonable interpretation in light of the specification in which they appear and the understanding of others skilled in the relevant art. *See* 37 C.F.R. § 42.200(b).

1. Proposed Constructions

Petitioner proposes constructions for "openly distributing," "environmental characteristics," and "internal rule." Pet. 5. Patent Owner disputes Petitioner's analysis, and provides its own constructions for the same claim terms. Prelim. Resp. 12–14. We determine that for purposes of this Decision, none of the disputed claim terms requires an explicit construction.

2. Remaining Claim Terms or Phrases

All remaining claim terms and phrases recited in the challenged claims are given their ordinary and customary meanings, consistent with the Specification, as would be understood by one with ordinary skill in the art, and need not be construed explicitly for purposes of this Decision.

B. Asserted Grounds of Unpatentability

Petitioner contends the challenged claims are unpatentable under 35 U.S.C. §§ 102 and 103 on the following specific grounds (Pet. 4):

Reference[s][2]	**Basis**	**Claims Challenged**
Digibox	§ 102(b)	1–6, 8–11, 13, and 21
Digibox and Stefik	§ 103(a)	7 and 14–20
Cooper	§ 102(b)	1–6, 8–11, 13, and 21
Cooper and Stefik	§ 103(a)	7 and 14–20

1. Unpatentability of Claims 1–6, 8–11, 13, and 21 Under 35 U.S.C. § 102(b) as Anticipated by Cooper

Petitioner contends that claims 1–6, 8–11, 13, and 21 are unpatentable under 35 U.S.C. § 102(b) as anticipated by Cooper. Pet. 4, 7–8, 30–60.

a. Cooper (Ex.1009)

Cooper describes a method and apparatus for distributing software objects from a producer to potential users which allows the user a temporary trial period without subjecting the software product to unnecessary risks of piracy or unauthorized utilization beyond the trial period. Ex. 1009, col. 2, ll. 28–33. The software object is preferably provided on a computer accessible media (e.g., magnetic media diskette, CD-ROM) along with a file management program. *Id.* at col. 2, ll. 33–38. The file management program is executed by a user controlled data processing system that

[2] The Petition relies on the following references: Olin Sibert, *et al.*, DigiBox: A Self-Protecting Container for Information Commerce, Proceedings of the First USENIX Workshop on Electronic Commerce New York, New York, July 1995 (Ex. 1008, "Digibox"); U.S. Patent No. 5,689,560 (Ex. 1009, "Cooper"); Mark Stefik, Letting Loose the Light: Igniting Commerce in Electronic Publication, March 1995 (Ex. 1015, "Stefik"). The Petition also relies on the Declaration of Mr. William R. Rosenblatt (Ex. 1001).

restricts access to the software object for a predefined and temporary trial period. *Id*. at col. 2, ll. 45–48. During the temporary trial mode of operation, the software object is temporarily enabled by decryption of the encrypted software object when the software object is called by the operating system of the user-controlled data processing system. *Id.* at col. 2, ll. 48–54. The file management program preferably prevents copying operations, so the encrypted software object is temporarily decrypted when it is called by the operating system. *Id*. at col. 2, ll. 54–58.

The trial software product is encrypted utilizing a temporary access product key, which is based upon one or more data processing system attributes and a derived machine identification value. Ex. 1009, col. 6, l. 65–col. 7, l. 4; col. 7, l. 51–col. 8, l. 8; col. 8, ll. 57–67; Figs. 3–4; *see id*. at col. 9, l. 1–col. 16, l. 5; Figs. 5–18. The file management program stores the temporary access product key on the user-controlled data processing system in a key file. *Id.* at col. 13, ll. 45–66. The key file includes the product key, customer key, machine identification number, and the trial interval data. *Id.* at col. 15, ll. 62–67; Fig. 18; *see id.* at col. 15, ll. 9–34; Figs. 14–15. When the encrypted software product is called for processing by the user-controlled data processing system, the encrypted file and the key file are fetched. *Id.* at col. 16, ll. 10–17; Fig. 19. The product key, customer key, and machine identification information included in the key file are applied as inputs to a decryption engine that outputs a real key. *Id*. at col. 16, ll. 20–32; Figs. 19–21. The real key and encrypted software object are input to the decryption engine which outputs the decrypted software object. *Id*. at col. 16, ll. 42–47; Fig. 23.

b. Claims 1–6, 8–11, and 13

Petitioner argues in the claim charts that Cooper discloses "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," as recited in claim 1. Pet. 34. Petitioner asserts the claimed "rules defining access rights to the data" corresponds to copy prevention and user interval rules enforced with keys, and the claimed "access mechanism" corresponds to Cooper's file management program. *Id.; see id.* at 30. Petitioner appears to equate the claimed "unprotected form of the protected data portions" to Cooper's disclosure of "decryption of the encrypted software object." *Id.* at 34 (quoting Ex. 1009, col. 2, ll. 45–57).

The Petition does not explain sufficiently how Cooper discloses rules defining access rights to the data, and how Cooper discloses each and every access to the decrypted software object (i.e., an unprotected form of the protected data portions) is limited in accordance with the rules as enforced by the file management program (i.e., access mechanism). The quotations from Cooper provided in the claim chart disclose the "file management system preferably prevents copying operations." *Id*. at 34 (quoting Ex. 1009, col. 2, ll. 45–57). However, the Petition does not explain sufficiently how Cooper's preferable prevention of copying operations discloses rules defining access rights to the data, and how Cooper discloses each and every access to the decrypted software object (i.e., unprotected form of the protected data portions) is limited in accordance with Cooper's preferable prevention of copying operations. The Petition also does not provide evidence sufficient to demonstrate that Cooper discloses "user interval rules," as asserted by Petitioner. *See id.* Instead, Cooper discloses trial

interval data encrypted to a key. *See* Ex. 1009, col. 15, ll. 4–20. The Petition does not explain sufficiently how Cooper's trial interval data encrypted to a key discloses rules defining access rights to the data, and how Cooper discloses each and every access to the decrypted software object (i.e., unprotected form of the protected data portions) is limited in accordance with trial interval data encrypted to a key as enforced by the file management program (i.e., access mechanism).

Accordingly, on the record before us, we determine the Petition does not establish a reasonable likelihood that Petitioner would prevail in showing that Cooper anticipates claim 1, and claims 2–6, 8–11, and 13, dependent therefrom.

c. Independent Claim 21

Petitioner argues in the claim charts that Cooper discloses "rules defining access rights to the data," and "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," as recited in claim 21. Pet. 57–60. Petitioner asserts the claimed "rules defining access rights to the data" corresponds to Cooper's disclosure of trial interval data encrypted to the product key (i*d.* at 57–59), and Cooper's disclosure of preferable prevention of copying operations (*id*. at 60 (quoting Ex. 1009, col. 2, ll. 45–57); *see id*. at 30). Petitioner further asserts the claimed "access mechanism" corresponds to Cooper's file management program (*id.* at 57–59), and the claimed "unprotected form of the protected data portions" corresponds to Cooper's disclosure of "decryption of the encrypted software object" (*id*. at 60 (quoting Ex. 1009, col. 2, ll. 45–57)).

For similar reasons as those explained above addressing claim 1, the Petition does not explain sufficiently how Cooper discloses rules defining access rights to the data, and how Cooper discloses controlled access to the decrypted software object (i.e., an unprotected form of the protected data portions) is provided only in accordance with the rules as enforced by the file management program (i.e., access mechanism). The quotations from Cooper provided in the claim chart disclose the "file management system preferably prevents copying operations." Pet. 60 (quoting Ex. 1009 col. 2, ll. 45–57). However, the Petition does not explain sufficiently how Cooper's preferable prevention of copying operations discloses rules, and how Cooper discloses controlled access to the decrypted software object (i.e., unprotected form of the protected data portions) is provided only in accordance with Cooper's preferable prevention of copying operations. The quotations from Cooper provided in the claim chart also disclose trial interval data 374 input to a product key encryption engine 375. Pet. 59 (quoting Ex. 1009, col. 15, ll. 4–20). However, the Petition does not explain sufficiently how Cooper's trial interval data 374 encrypted to the key discloses rules defining access rights to the data, and how Cooper discloses controlled access to the decrypted software object (i.e., unprotected form of the protected data portions) is provided only in accordance with the trial interval data encrypted to the key as enforced by the file management program (i.e., access mechanism).

Accordingly, on the record before us, we determine the Petition does not establish a reasonable likelihood that Petitioner would prevail in showing that Cooper anticipates claim 21.

2. Unpatentability of Claims 1–6, 8–11, 13, and 21 Under 35 U.S.C. § 102(b) as Anticipated by Digibox

Petitioner contends that claims 1–6, 8–11, 13, and 21 are unpatentable under 35 U.S.C. § 102(b) as anticipated by Digibox. Pet. 4, 7–30.

a. Digibox (Ex. 1008)

Digibox describes that DigiBox is a foundation technology within InterTrust Virtual Distribution Architecture. Ex. 1008, 7. DigiBox provides a secure container to package information so that the information cannot be used except as provided by the rules and controls associated with the content. *Id.* InterTrust rules and controls specify what types of content usage are permitted. *Id*. DigiBox is a container for both digital property (content) and controls. *Id.*

b. Claims 1–6, 8–11, 13 and 21

Petitioner asserts in the claim charts that Digibox teaches "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," as recited in claim 1, and "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," as recited in claim 21. Pet. 12, 29–30. In support of these assertions, Petitioner provides, in the claim charts, quotations from Digibox, and citations to certain paragraphs of Mr. Rosenblatt's Declaration. *Id.* at 12, 29–30 (quoting Ex. 1008, 7–8; citing Ex. 1001 ¶¶ 74–77, 200–203).

We agree with Patent Owner that the Petition only addresses limited or controlled access to protected (i.e., encrypted) forms of the data, and does not explain how Digibox discloses limited or controlled access to

unprotected forms of the protected data as enforced by an access mechanism, as required by claims 1 and 21. Prelim. Resp. 15, 17, 19–21; *see* Pet. 9, 12, 29–30. For example, Petitioner asserts that Digibox provides the following teachings: (1) portions of the sent data may be encrypted or protected; (2) the encrypted (i.e., protected) portions of data are sent in a secure container (i.e., a "DigiBox"), so that the information cannot be used except as provided by the rules and controls associated with the content, and (3) when a recipient attempts to access the data, access is through the user's computer's storage manager, which will access the *encrypted* (i.e., protected) data on the DigiBox in accordance with the rules and controls. *Id.* at 9 (quoting Ex. 1008, 8–9) (emphasis added); *see id*. at 12 (quoting Ex. 1008, 7–8), 29–30 (quoting Ex. 1008, 8).

Accordingly, on the record before us, we determine the Petition does not establish a reasonable likelihood that Petitioner would prevail in showing that Digibox anticipates claims 1–6, 8–11, 13, and 21.

3. Unpatentability of Claims 7 and 14–20 Under 35 U.S.C. § 103(a) as Obvious Over Digibox and Stefik, and Over Cooper and Stefik

Claims 7 and 14–20 ultimately depend from claim 1. As applied by Petitioner, the teachings of Stefik do not remedy the deficiencies of Digibox and Cooper in disclosing all of the limitations of claim 1. *See* Pet. 7–8, 10, 16–17, 22–28, 31–32, 40–43, 49–57. Therefore, on the record before us, we determine the Petition does not establish a reasonable likelihood that Petitioner would prevail in showing that claims 7 and 14–20 would have been obvious over Digibox and Stefik, and over Cooper and Stefik.

III. CONCLUSION

Based on the record before us, the information presented in the Petition does not demonstrate that there is a reasonable likelihood that Petitioner would prevail in showing that claims 1–11 and 13–21 are unpatentable.

IV. ORDER

Accordingly, it is ORDERED that the Petition for *inter partes* review is DENIED.

PETITIONER:

Kenneth R. Adamo
Brent Ray
Joel Merkin
Eugene Goryunov
KIRKLAND & ELLIS LLP
kenneth.adamo@kirkland.com
brent.ray@kirkland.com
jmerkin@kirkland.com
eugene.goryunov@kirkland.com

PATENT OWNER:

Lori Gordon
Omar Amin
STERNE, KESSLER, GOLDSTEIN & FOX PLLC
lgordon-PTAB@skgf.com
oamin-PTAB@skgf.com