BESCHWERDEKAMMERN BOARDS OF APPEAL OF CHAMBRES DE RECOURS
DES EUROPÄISCHEN   THE EUROPEAN PATENT DE L'OFFICE EUROPÉEN
PATENTAMTS   OFFICE   DES BREVETS

Internal distribution code:
(A) [-] Publication in OJ
(B) [-] To Chairmen and Members
(C) [-] To Chairmen
(D) [X] No distribution

Datasheet for the decision
of 27 January 2023

Case Number: T 0366/20 - 3.5.07

Application Number: 11156328.4

Publication Number: 2492825

IPC: G06F17/30

Language of the proceedings: EN

Title of invention:
Efficient multiple identity system for media files

Applicant:
BlackBerry Limited

Headword:
Multiple identity system for media files/BLACKBERRY Limited

Relevant legal provisions:
EPC Art. 56
RPBA 2020 Art. 13(2)

Keyword:
Admissibility - sole request (yes)
Inventive step - sole request (no)

Decisions cited:
G 0001/19

Catchword:

No technical effect of the distinguishing features over the disclosure of document D1 can be derived over the whole scope of claim 1 (see decision G 1/19 of 10 March 2021, sections 82 and 95).

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Case Number: **T 0366/20 - 3.5.07**

D E C I S I O N
of Technical Board of Appeal 3.5.07
of 27 January 2023

Appellant: (Applicant)	BlackBerry Limited 2200 University Avenue East Waterloo, ON N2K 0A7 (CA)
Representative:	Murgitroyd & Company Murgitroyd House 165-169 Scotland Street Glasgow G5 8PL (GB)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 2 October 2019 refusing European patent application No. 11156328.4 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chair	J. Geschwind
Members:	C. Barel-Faucheux
	M. Jaedicke

Summary of Facts and Submissions

I.   The appellant (applicant) appealed against the
        examining division's decision to refuse European patent
        application No. 11156328.4 (published as EP 2492825).

II.   The documents cited in the contested decision included:
        D1:   US 2005/0004941 A1, published on 6 January 2005

III.   The examining division decided that claims 1 and 6 of
        both the main request and the first auxiliary request
        lacked an inventive step over document D1, contrary to
        the requirements of Article 56 EPC, and that neither
        claim 1 nor claim 6 of the first auxiliary request
        fulfilled the requirements of Article 123(2) EPC.

IV.   In its statement of grounds of appeal, the appellant
        requested that the contested decision be set aside and
        that a patent be granted on the basis of the main
        request considered in the contested decision and re-
        submitted with the statement of grounds of appeal or,
        alternatively, on the basis of either the first or
        second auxiliary requests submitted with the statement
        of grounds of appeal.

V.   In a communication accompanying the summons to oral
        proceedings, the board expressed its preliminary view
        that claim 1 of the main request lacked clarity under
        Article 84 EPC, that there appeared to be no reason for
        admitting the first and second auxiliary requests under
        Article 12(6) RPBA 2020, that the subject-matter of
        claim 1 of the first auxiliary request appeared to
        infringe the requirements of Article 123(2) EPC, and
        that the subject-matter of claim 1 of the main request
        and of the first and second auxiliary requests lacked

an inventive step over document D1 under Article 56
EPC.

VI.   With a letter dated 14 December 2022, the appellant
filed a new first auxiliary request together with
further arguments concerning the clarity and inventive
step of the main request and the new first auxiliary
request.

VII.   During the oral proceedings, the appellant withdrew the
main request and replaced it with the new first
auxiliary request as the sole request.

VIII.   The appellant requests that the decision under appeal
be set aside and that a patent be granted on the basis
of the set of claims of the sole request on file.

IX.   The sole request on file has been broken down into
features by the board in section 3 of the Reasons
below.

X.   The appellant's arguments, where relevant to the
decision, are discussed in detail below.

Reasons for the Decision

Application

1.   The application relates to devices and methods for
managing the identity of media content data (see
paragraph [0001] of the description as originally
filed). It is common for the same media content to be
available from numerous sources, each of which may use
a different proprietary identification scheme for
describing, via the use of metadata, its creator or the

artist's name, the (song) title, track number, or other associated information (see paragraph [0003]).

2.   The application states that, in addition to the user experiencing frustrating delays while a duplicate file is being downloaded, redundant downloads to the same mobile device place an unnecessary burden on wireless network infrastructures. Furthermore, storing duplicate media content files that are referenced with different identifiers unnecessarily uses the limited storage space within a mobile device. Moreover, managing the identities of these duplicate files is tedious, time-consuming, and annoying for the user of the mobile device (see paragraph [0004]).

Sole request

3.   Claim 1 of the sole request reads as follows (broken down into features by the board):
        A   A client node, comprising:
        B   a database comprising a plurality of media content data files;
        C   a database comprising local identification data and metadata both associated with the plurality of media content data files; and
        D   processing logic for performing media content identity management operations,
        E   the processing logic used by the client node to reconcile the identity of individual media content data files of the plurality of media content data files,
        F   the processing logic configured to perform:
        F1   selecting a media content data file stored in a media content data source;

F2   receiving a first set of metadata associated with
     the selected media content data file from the
     media content data source;

F3   providing the first set of metadata to a server
     node;

F4   receiving from a server node a first master
     identifier corresponding to the first set of
     metadata;

F5   processing the first master identifier to identify
     whether there is any second master identifier
     stored in the database of local identification
     data and metadata that matches the first master
     identifier; and

F6   acquiring the selected media content data file in
     response to determining that there is no second
     master identifier stored in the database of local
     identification data and metadata matching the
     first master identifier.

4.   *Admissibility - sole request*

5.   During the oral proceedings, the board admitted the new
        first auxiliary request, which became the sole request
        on file. The exceptional circumstances for admitting
        said request under Article 13(2) RPBA 2020 were that
        the board had raised new objections under Article 84
        EPC against what was then the pending main request in
        sections 9 to 13 of the board's communication, and the
        new first auxiliary request overcame these objections.

6.   *Inventive step – claim 1*

7.   D1 was considered by the examining division to be the
        closest prior art to the subject-matter of claim 1 of
        the pending main request. The board also considers it
        to be the closest prior art to the subject-matter of

claim 1 of the sole request and the appellant has not contested this.

8.   In a first embodiment of document D1, a network crawler 200 is connected to a server 210 and is arranged to obtain multimedia objects that clients are sharing over a file sharing network 100. It can contact the server 110/210 to obtain a list of all the available multimedia objects, and then directly access all the individual clients 101 to 105 to download all the available multimedia objects (see paragraph [0042] together with Figures 1 and 2). The crawler 200 also obtains a set of metadata for the multimedia object from the client from which it obtains the multimedia object itself (see paragraph [0044]). Having downloaded a multimedia object, the crawler 200 then computes a fingerprint from the multimedia object (see paragraph [0045]).

9.   In a sub-embodiment of the first embodiment, the server 210 maintains the database 211. A networking module 301 in the server 210 receives the computed fingerprint and the obtained set of metadata from the crawler 200. A verifying module 302 of the server checks whether the received fingerprint is already present in the database 211. If the received fingerprint is already in the database 211, the verifying module 302 submits the set of metadata to a Database Management System (DBMS) backend module 303, which updates the database 211 to associate the set of metadata with the fingerprint already in the database 211. If the received fingerprint is not already in the database 211, the verifying module 302 submits the computed fingerprint and the obtained set of metadata to the DBMS back-end module 303, which adds the fingerprint and the set of metadata, associated with each other, to the database

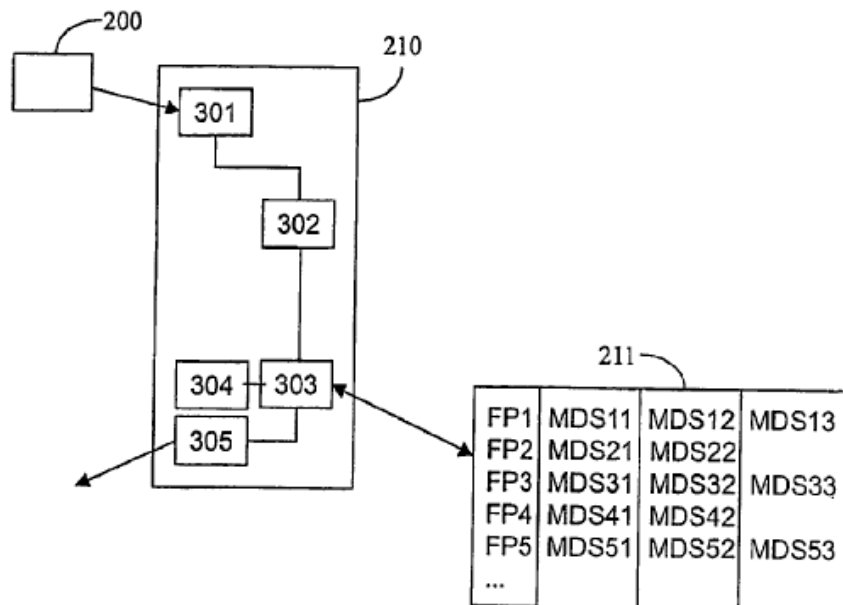211 (see paragraphs [0050] and [0051] and Figure 3 reproduced below).

FIG.3

10.   Once the definite set of metadata for a particular fingerprint has been determined (i.e. once a "sufficient" number of sets of metadata are associated with said particular fingerprint in the database 211), the definite set of metadata can be fed back to the clients to enable them to update their metadata for the song in question (see paragraph [0065]; emphasis by the board). The server 210 can make at least a portion of the database 211 available to others by offering a search interface 305 through which clients can submit a fingerprint and receive a set of metadata in return (see paragraph [0066], emphasis by the board).

11.   A fingerprint of the method of document D1 can thus be equated to a "master identifier" according to claim 1, while a set of metadata in document D1 corresponds to a "set of metadata" according to claim 1.

12.   One of the clients 101 to 105 of document D1 can be
        equated to a "client node" of claim 1. In document D1,
        the multimedia objects that a client is sharing over a
        file sharing network, together with their respective
        set of associated metadata, are stored in a (local)
        database in the client. Indeed, paragraph [0069] states
        that it is also possible to maintain the database with
        fingerprints and sets of metadata in a distributed
        fashion in one or more of the file sharing clients 101
        to 105. The local "fingerprint" would then correspond
        to the "local identification data" according to claim
        1.

13.   Each (file sharing) client of document D1 also
        comprises some "processing logic" for performing media
        content identity management by using a database 405
        comprising fingerprints and associated sets of metadata
        for each shared multimedia object stored in storage 403
        (see paragraphs [0069] to [0073] and Figure 4).

14.   Thus, document D1 discloses features A to D of claim 1
        of the main request. It also discloses features F, F1
        and F2 when retrieving a multimedia object as a "media
        content data file" according to claim 1 from the
        database of another client node sharing its media
        content as a "media content data source" as according
        to claim 1.

15.   Paragraph [0073] of document D1 reads: "A fingerprint
        for a multimedia object can be computed while that
        object is being downloaded, since only a relatively
        small portion of the object is necessary to compute a
        fingerprint. [...] If during this process it is
        determined that the fingerprint is already in the
        database 405, it is very likely that the user already

has a copy of this particular multimedia object in his
possession. The user could then be warned, so that he
could abort the downloading".

It is well known to the skilled person that when the
downloading of a file to a storage place is aborted
(for example because the user already has a copy of
this particular multimedia object), the incompletely
downloaded file is usually removed from this storage
place. Thus, document D1 additionally discloses, in the
sub-embodiment in which the database with fingerprints
and the sets of metadata are maintained in a
distributed fashion (see D1, paragraphs [0069] to
[0073]), feature F6 and the following features (wherein
the parts in italics are not present in claim 1 and the
crossed out parts are present in claim 1 but not in
document D1):

F4' receiving from a server node *a part of a media content
     data file to compute* a first master identifier
     ~~corresponding to the first set of metadata~~ (the another
     client acting as a server node);

F5' ~~processing~~ *using* the first master identifier to
     identify whether there is any second master identifier
     stored in the database of local identification data and
     metadata that ~~matches~~ *is the same as* the first master
     identifier; and

16. Therefore, the board is of the opinion that the
     distinguishing features of claim 1 of the main request
     over document D1 are feature E (in particular "to
     reconcile the identity of individual media content data
     files") and, in essence, features F3 to F5.

17.   In reply to the board's communication and during the
        oral proceedings before the board, the appellant argued
        that the objective technical problem to be solved was
        "how to provide, at a client node, a more efficient
        non-duplicate downloading and file identity
        reconciliation".

18.   The appellant argued that this corresponded to an
        advantageous technical effect because even if a small
        portion of the selected file could be sufficient to
        derive a file identifier at the client node (as in the
        case of the fingerprints disclosed in D1), and even if
        this portion of the file could be removed from the
        client node if the download was aborted, a small
        portion of a large selected file (e.g. a video file)
        still corresponded to a large amount of data relative
        to the limited storage capabilities of the client node
        (this could cause problems or inefficiencies of
        operation of the client node even with a limited
        storage time).

19.   The appellant argued in its statement of grounds that,
        according to claim 1 of the pending main request, a
        first master identifier was fetched from a remote
        server node on the basis of metadata associated with
        the selected media content data file.

19.1   According to D1, the fingerprint for a multimedia
        object was computed while that object was being
        downloaded (and reference was made to paragraph
        [0073]). Once the fingerprint was computed, it could be
        compared to fingerprints stored in the local database
        of the user, and accordingly the user could be warned
        if a matching fingerprint was found. Therefore, with
        the method presented in document D1, a portion of the
        selected multimedia object would need to be downloaded

to the personal computer of the user before the
fingerprint for the selected multimedia object could be
computed and compared to the fingerprints stored in the
local database. In the case where a duplicate object
was identified in the local database after the
computation of the fingerprint, the downloaded portion,
irrespective of its size, would have unnecessarily used
up storage space in the user's personal computer device
and placed an undue burden on the bandwidth of the file
sharing network.

20.   According to the appellant, the claimed solution
        provided downloading of non-duplicate media files along
        with reconciliation of file identities based on
        received metadata of media files selected for possible
        download. By contrast, D1 taught a solution for
        downloading of non-duplicate media files based on
        received initial portions of the files selected for
        possible download and was concerned at most with
        reconciling metadata based on file identifiers
        (according to paragraphs [0051] to [0064] of document
        D1, different metadata associated with different
        instances of the same file were aggregated to a
        respective file identifier, and then filtered to elect
        a definite set of metadata for the file identifier). As
        a further advantage, the claimed solution avoided
        conflicts due to having copies of the same file
        identifier (associated with respective copies of the
        same file) that were locally stored in association with
        the same or similar metadata.

21.   However, the board is of the opinion that no technical
        effect of the distinguishing features can be derived
        over the whole scope of the claim (see decision G 1/19
        of 10 March 2021, sections 82 and 95).

21.1   The board first notes that the "local identification
        data" are not further defined in claim 1 (see feature
        C). They are also only stored in a database of the
        client node but are not further used by the processing
        logic stipulated in, or the client defined by, claim 1.

21.2   Concerning feature F5, the board also notes that the
        expression "matching", while encompassing "being
        identical to", does not exclude other types of
        correspondences such as "having some similarity",
        "being analogous to", "being paired with", *etc.*

21.3   Moreover, the board is of the view that claim 1 does
        also not exclude the fact that the selected media
        content data file is acquired when there is a second
        master identifier stored in the database of local
        identification data and metadata matching the first
        master identifier (see feature F6).

21.4   During the oral proceedings, the appellant stated that
        only the first set of metadata were received, and not
        the selected media content data file (see features F1
        and F2). The metadata were associated with the media
        content data files but outside of the media content
        data files.

21.4.1 The board notes that it is stated in the description of
        the application that a proprietary identification
        scheme based on an Extensible Markup Language (XML)
        file schema or ID3 tags accommodates metadata such as
        the artist's name or the creator, track number, song
        title, or "other associated information" (see paragraph
        [0003] of the description as originally filed). During
        the oral proceedings, the board informed the appellant
        that a multimedia file in some cases comprised metadata
        associated with the file. Moreover, D1 discloses that,

often, the set of metadata is included in or with the
multimedia object, so that obtaining the set of
metadata happens automatically when obtaining the
multimedia object. For instance, a multimedia object
with music in the popular MP3 format often contains
metadata as an ID3 tag at the end of the object
(paragraph [0044] of document D1). D1 teaches that a
fingerprint (or "(robust) hash") of a multimedia object
is a representation of the "most relevant perceptual
features" of the object in question: thus, for two
multimedia objects to be considered the same, their
fingerprints should be the same (paragraph [0002] of
document D1). This concurs with the appellant's
argument that according to document D1, the fingerprint
could be computed based on the extraction of time-
frequency characteristics of the multimedia object,
which were unique for each multimedia file (see the
board's communication, section 25.2).

21.5   The appellant argued during the oral proceedings that
        the set of metadata were used as an index for
        retrieving a first master identifier based on
        associations between master identifiers and metadata at
        the server node. Furthermore, the appellant argued that
        according to document D1, the fingerprint could be
        computed based on the extraction of time-frequency
        characteristics of the multimedia object, which were
        unique for each multimedia file, and not based on
        metadata. In the method of document D1, the metadata
        was only an optional feature and did not contribute to
        the computation of the fingerprint.

21.6   The board notes that in claim 1 of the sole request,
        the metadata does not appear to contribute to the
        computation of the "master identifier" (as a
        "fingerprint"). Feature F4 recites "receiving from a

server node a first master identifier corresponding to
the first set of metadata", but this can be interpreted
as using the first set of metadata as an index for
retrieving a first master identifier. This appears to
be confirmed by the appellant, which stated that the
application disclosed a mechanism to generate and
maintain master identifiers at the server node, whereby
upon collection of a media file from a respective
source along with its associated metadata:
- the server node searched to identify pre-existing
metadata corresponding to the media file;
- if no pre-existing metadata were identified, the
server node generated the master identifier and
associated it with the collected metadata; and
- if pre-existing metadata were identified, the server
node identified a pre-existing master identifier
associated with the identified pre-existing metadata
and re-indexed this identified pre-existing master
identifier to both the pre-existing and newly collected
metadata.

Thus, the server nodes could maintain master
identifiers each associated with respective sets of
metadata belonging to different instances of the same
file (the appellant referred to paragraphs [0051] and
[0052], paragraphs [0060] to [0062] and Figure 6 of the
application).

21.7   However, claim 1 does not define how the "first master
identifier" received from a server node corresponds to
the "first set of metadata" provided by the client to
this server node (see feature F4). Since the first
master identifier seems to be determined based only on
the metadata, and since the metadata may be incomplete
or incorrect or otherwise not identifying for the media
content or may not capture differences in actual

content of the media content data files (for example due to different versions of the same song, movie *etc.*) the result of the claimed method seems to be essentially unpredictable with respect to the detection of duplicate media content files over the whole scope of the claim.

21.8   Moreover, the claim does not define what "processing" is performed on the first master identifier to identify whether a second master identifier is stored in the database of local identification data and metadata that matches the first master identifier (see feature F5).

21.9   Since there is no technical effect over the whole scope of the claim, no technical problem is solved over the whole scope of the claim and the claimed method therefore lacks an inventive step (Article 56 EPC).

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chair:

S. Lichtenvort   J. Geschwind

Decision electronically authenticated