

Improvements in and relating to the distribution of content

The present invention relates to the distribution of content over networks,
5 particularly although not exclusively content having digital rights such as
copyright therein.

A particular challenge to the content generating community which includes
record companies, publishers and other right holders, is the ease with which
10 digital content may be disseminated particularly over networks. This ease of
dissemination is also coupled with the fact that there is little or no degradation
in the quality of the content despite repeat copying and forwarding of the
content in its original format. Thus, unauthorised copies of copyright context
will meet the same high expectations of consumers in relation to the
15 authorised content.

Consequently, right holders have been reluctant to make their content
available for distribution over networks. In a parallel development, efforts are
presently being made to prevent or at least restrict the ability of purchasers of
20 such content to make further copies thereof.

Where content has been made available for distribution over networks,
various proposals have been made to counter the loss in revenue to right
holders. Broadly, these have constituted, on the one hand, the creation of
25 technical barriers to unauthorised copying of content and on the other hand,
the development of transactional controls. In many cases both approaches
have been used in tandem to attempt to strictly control the distribution of
content to authorised recipients namely those users who have paid the
appropriate fee to the right holder. The implementation of such techniques
30 does require significant processing power and requires specific hardware
and/or software features in a terminal. Indeed, as the sophistication of those
seeking unauthorised access to content increases, the demands for

processing power will only increase. Furthermore, as many proprietary approaches exist there result in a multiplicity of hardware and software features in different terminals. As a result of the ensuing poor level of interoperability and concomitant fragmentation of the market, right holders are
5 reluctant to invest in making content available.

Thus, according to one aspect of the present invention, there is provided a content distribution control system comprises a network having at least one terminal connected thereto, a content creation tool operable to assign indicia
10 representative of a pre-determined level of control of said content, said content being subsequently made available to said network and said at least one terminal being responsive to said indicia to permit operations in relation to said content received from said network.

15 The content creation tool may be an application resident on a terminal thereby allowing users to generate their own content such as ringtones and to assign a desired level of protection to that content. At the other end of the scale, a publisher might utilise such a tool to make their works available over a network in which case a level of control for such content may be assigned.
20 The content need not be provided in an electronic format but could be distributed on Compact Disc (CD) or Digital Versatile Disc (DVD), the only requirement being that the indicia remain with the content when it is transferred to other media including uploading the content to a network. Thus, the right holder is assured that his intentions regarding dealings with the
25 content are preserved. To deter unauthorised dealings in the content, the indicia may be encrypted and/or encryption may be utilised over those channels of communication via which the content is distributed. The simplicity of the approach facilitates its implementation on all platforms including relatively thin clients such as mobile terminals unsuitable for implementing the
30 computationally and resource intensive demands of prior art content distribution systems. Thus there is no need to implement blanket prohibition

of the forwarding of right holder's content from terminals such as hitherto been the case with ringtones for example.

According to another aspect of the present invention, there is provided a
5 terminal having a first memory into which content is receivable, a second memory and a user interface operatively associated with said memories, such that a set of operations of said user interface in relation to said content received into said first memory is permitted by reference to said content, at least one of said operations permitted by said content being a transfer of said
10 content to said second memory, wherein a set of operations of said user interface in relation to said same content when received into said second memory is similarly permitted by reference to said content.

It will be recognised that because the user interface is responsible for
15 managing the operations permitted or allowed in respect of the content and that the content itself is otherwise unavailable to a typical user, there is no requirement for computationally and resource intensive cryptographic protection of the content. Preferably, the first memory is volatile with the result that content is not retained in the terminal unless the indicia permits
20 transfer of the content to the second non-volatile memory. However, the terminal may implement session level cryptography to protect the content during transit over the network.

According to a further aspect of the present invention, there is provided a
25 method of creating content for controlled distribution comprises defining indicia representative of respective levels of control of content, determining a level of control appropriate to said content and assigning indicia to said content in accordance with said determination.

30 Because the level of control may be set during the creation of content a right holder is able to set out at the outset his intention regarding the copyright status, for example, of that content. Attempts to defeat this intention by

removing such indicia may be actionable and thus the presence of the indicia acts as a form of legal tripwire which can be tested in cases of unauthorised use of the content. Furthermore, the indicia, by remaining intact during transfer of the content, ensures that the intentions of the right holder are retained even where the content is transferred between different media including physical devices such as Compact Discs and Digital Versatile Discs and electronic copies held on web servers, for example. The management of such rights is further enhanced as a user interface of a terminal or other device receiving such a content can be programmed to respond in a predetermined manner to content having particular indicia. Such a simplification of the management process reduces the computational and other resource requirements of a terminal.

According to a still further aspect of the present invention, there is provided a method of receiving content including indicia representative of allowable operations in respect of said content, which comprises receiving said content into a first memory, generating a list of allowable operations in relation to said content from said indicia and displaying said list to a user.

One at least of the allowable operations will be transferring the content to a second, non-volatile, memory. However, in some circumstances, for example, where the content is intended for promotional purposes, such a transfer will be prohibited by the indicia. In which case, the content would be deleted when the first volatile memory is purged or the terminal powered down. Consequently, the opportunity to seek to hack or otherwise carry out unauthorised activity in relation to the content will be denied.

In order to understand the present invention more fully, a number of embodiments thereof will now be described by way of example and with reference to the accompanying drawings, in which:

Figure 1 is a schematic view of a communication network in accordance with one aspect of the present invention;

Figure 2 is a diagrammatic view of a terminal for use with the network of Figure 1 in accordance with a further aspect of the invention;

5 Figure 3 is a diagrammatic view of a datagram for use with the network of Figure 1 in accordance with a further aspect of the invention;

Figure 4 is view of information shown on a display of the terminal of Figure 2; and

10 Figures 5a, 5b and 5c are all views of different information shown on a display of the terminal of Figure 2.

Referring to Figure 1, there is shown a communication network 1 to which a plurality of terminals 3 has access. The network 1 has interworking
15 connections 5 to external networks 7 including the Internet 9. In addition to locally created content and through these external connections 5 allow content to enter the communication network 1.

Referring in particular to Figure 2, a terminal 3 for use with the network 1 is
20 provided with a processor 9, memory 11 and data input 13 and output devices 15. The memory 11 includes a cache 17 into which data is received from the network 1. The cache 17 operates by retaining data on a temporary basis which is being used by the terminal 3 thereby preventing repeat requests from the terminal 3 for the network 1 to deliver the same data. At the end of a
25 communication session and/or when data has not been accessed for a predetermined time period, the cache 17 is emptied. The terminal 3 is provided with a User Interface (UI) 19 to namely an application which controls reprocessing co-ordinate the activities of the terminal 3 in response to inputs from a user and/or the network 1.

30

The terminal 3 may be connected to the network 1 in a conventional manner. Thus a fixed terminal may be connected by a modem 21 connected to the

network, for example. In the case of a mobile terminal, the connection may be over an air interface 25, in which case the terminal 3 will include the appropriate well known additional elements required to perform this function. The techniques for connection of such terminals to the network 1 will be readily apparent to those skilled in the art.

As has already been mentioned, content may enter the network 1 from externally connected content providers 22 or the network 1 itself may incorporate content providers 29 including, but not limited to, the terminals 3 themselves. As shown in Figure 3, content 31 is encapsulated in a datagram 33 formatted in accordance with the frame type of the protocol the network 1 is operating. Typically, the datagram 33 has a header portion 35 which is provided with fields 37, 39, 41 containing a destination address 43 and respectively the address 45 of the sender's device and an initial router address 47 determined from a look-up table or similar held by the terminal 3. In the case of a so-called second generation Public Land Mobile Network (PLMN) as exemplified by GSM, the content 31 may be in the form of text or ringtone data carried by a Short Message (SM). In which case the destination address 43 will be the receiving terminal's telephone number, the sender's address 45 the sending terminal's telephone number and the initial router address 47 the Short Message Service Centre telephone number. The content 31 itself is conveyed in a payload portion 49 of the datagram 33.

The content 31 contains a value indicative of a control or copyright class 51 to which belongs. This may take the form of a value placed in a sub division 50 of the payload portion 49 or elsewhere within the content 31. The class 51 is initially assigned to a contents 31 by an application under the control of the right holder or a party authorised by him within the function of a service creation tool (not shown). Such tools are commonly used to create personalisation material such as ringing tones, profile icons, picture messages, screen savers and digital images, to name but some possibilities. The digital rights associated with such material will vary and thus a suite of

options is available within the tool to set an appropriate level of protection. Each level of protection will place a different level of restriction on the use a recipient may make of the content 31. The indication of the class 51 may be performed by setting a bit to a corresponding state. Depending on the
5 resources available, the indication of class 51 may be used to deliver more detailed information relating to the content 31 with which it is associated.

One of the functions of the terminal UI 19 is to control the delivery of datagrams for a user as exemplified by the delivery of an SM to a mobile
10 terminal 3 connected to a GSM network 1, for example. When a datagram 33 is received by the terminal 3, it is placed in the cache 17 which is accessible to the UI but not otherwise accessible to a user operating the terminal 3 in a normal fashion. A UI function examines the payload portion 49 for a value indicative of the control class 51 applied to the content encapsulated by the
15 datagram 33. As previously mentioned, the value may be placed in a sub-division 50 within the payload portion 49 or indeed any other predetermined location within the datagram 33.

The value 51 is then compared by the UI function against a set of pre-existing
20 conditions each representing a set of allowable and prohibited operations in relation to the content 31. These correspond, of course, to those assignable by the content creation tool. If necessary, these conditions could be varied by a network operator in concert with a right holder, by delivering a new set of conditions to the terminal 3 to reflect changes in a content creation tool.

25 By way of example, three conditions and corresponding control value or other indicia may be established in relation to user operations that may be carried out in relation to content 31. Firstly, that the content 31 may be viewed only; secondly, that the content 31 may be viewed and saved locally within the
30 terminal 3 ; and thirdly, that the content may be viewed, saved locally within the terminal 3 and freely forwardable over the network 1 such as, for example, to other terminals 3.

In use, a datagram 33 such as a SM will be received by the terminal 3 to which it is directed and the datagram 33 stored temporarily in the cache 17. The UI function 19 will subsequently display to the user a message (Figure 4) indicating that a SM, such as a ringtone, has been received. The user will be
5 given the option at this stage to either open 59 the SM or to discard it by exiting 61 the UI function. In this latter case 61, the UI function will issue an instruction to clear the cache 17.

Presuming the user elects to open 59 the SM one of the three displays
10 illustrated in Figures 5a, 5b and 5c will be displayed by the UI function 19 in accordance with the indicia 51 set by the content creation tool. The nature of the display will depend on the indicia 51 associated with the content 31. Thus, the operations allowed to a user might include, in the case of a ringtone, the playing the ringtone, saving the ringtone for future local use,
15 forwarding the ringtone to another terminal and lastly erasing the ringtone. For different forms of content 31, it will be appreciated that alterations may be made to the operations available to the user although the operation to save and forward will always be present although perhaps prohibited under certain classes of control.

20

Figure 5a represents a terminal 3 display 15 to a user in which the first class of copyright control has been placed upon the content 31. Thus, the options to save 55, forward 57 or erase 63 the SM have been greyed out leaving the only option open to the user of playing 53 the ringtone. Such a copyright
25 class would allow a user to access content for promotional or investigatory purposes only. Under this classification, there is no option to retain the SM for later local use or to forward it. Thus, once the UI function 19 has been exited through the requisite menu selections or indeed the terminal has been powered down, the cache 17 is cleared and the SM is no longer available.
30 Clearly, there is no need to enable the option to erase the content 31 as this will occur in any case on exiting the UI function or switching off the terminal.

Figure 5b represents a terminal 3 display 19 in which a second class of copyright control has been placed upon the content 31. Thus, the option to forward 57 the content to another terminal has been greyed out leaving the options of playing 53 or saving 55 the content 31 locally are available to the user. Such a control class would allow a user access to content 31 he has purchased without melody the right to disseminate it further.

Finally, Figure 5c represents a terminal 3 display 19 in which a third class of copyright control has been placed upon the content 31. Thus, the options to forward 57, save 55 and play 53 together with the option to erase 63 the content 31 are available to the user. Such a class would be the default setting for content 31 not attributable to any right holder.

Depending on the class and options allowed to a user, selection from a menu will result in the UI carrying out the relevant action, which in the case of saving 55 the SM will result in the content 31 being transferred from the cache 17 into the memory non-volatile 11 of the terminal 3. The remaining options result in the UI operating directly on the content held in the cache 17.

It will be appreciated that by placing the copyright control information in a portion 36 of the datagram 33 which remains in the cache 17, at least until it is saved to the terminal menus 11, provides basic protection against hacking. Furthermore, once the content 31 has been stored locally, separate security measures may be employed to guard against hacking the copyright control class 51 of the stored content.

Nevertheless, to protect against more sophisticated hacking, the header portion may further include a checksum value of the entire content held in the payload portion 36. The UI function could initially determine whether the checksum was correct and if not this would be indicative of either data corruption during the transmission process or an attempt to make an unauthorised change to the copyright control class 51. For example, a

10

checksum could consist of a simple sum of the sub division 34 and content 31 the payload 34 divided by a pre-selected prime number. The remainder would then serve as an indicator of the integrity of the copyright control class 51.

5

Further security measures such as those necessary to avoid so-called man in the middle attacks or modification of the terminal itself could be defeated by utilising the Public Key Infrastructure (PKI) and a suitable cryptographic technique. Thus, a PKI based technique would be utilised to establish a
10 secure connection between a pair of terminals 3 or a terminal 3 and a content provider between which a datagram 33 containing copyright content would travel.

Claims

1. A content distribution system comprising
a network (1), and
a terminal (3) with a user interface (19) to perform a plurality of individual user selectable operations for data content (33) supplied to the terminal through the network, said operations being controlled in dependence on the data content **characterised by**
a content creation tool (22, 29) operable to assign and include indicia data (51) in data content (33) to be supplied through the network to the terminal, the indicia data indicating which of the plurality of individual user selectable operations are permitted for the data content by user selection at the terminal,
operation of the user interface of the terminal being controlled for the data content by the indicia data included therein such that said user selectable operations are each individually enabled or disabled in dependence on the indicia data.
2. A system as claimed in claim 1 comprising a communications link providing said tool with access to the network.
3. A terminal (3) to receive data content (33) through a network, comprising a memory (11, 17) for storing received data content, and a user interface (19) to perform a plurality of individual user selectable operations for the data content and said operations being controlled in dependence on the data content **characterised by**
the user interface being responsive to data content supplied to the terminal that includes indicia data (51) indicating which of the plurality of individual user selectable operations are permitted for the data content by user selection at the terminal, and
the operation of the user interface is controlled for the data content (33) by the indicia data (51) included therein such that said user selectable operations are each individually enabled or disabled in dependence on the indicia data.

4. A terminal as claimed in claim 3 wherein said indicia data is included in the payload portion (49) of a datagram (33) containing said data content.
5. A terminal as claimed in claim 3 or 4 wherein the indicia data (51) is encrypted.
6. A terminal as claimed in claim 3, 4 or 5 wherein the terminal (3) is a mobile telephone handset.
7. A terminal as claimed in claim 6 configured to be supplied with the data content in the form of a short message (SM).
8. A terminal according to claim 6 configured to be supplied with data content that comprises a ringtone.
9. A terminal as claimed in any one of claims 3 to 8 wherein the user interface is operable to perform viewing, storing, deleting and forwarding as user selectable operations for the data content.
10. A terminal as claimed in any one of claims 3 to 9 wherein said terminal comprises a volatile memory (17) and a non-volatile memory (11) and said user selectable operations for the data content include transferring the data content (33) from said volatile memory (17) to said non-volatile memory (11).
11. A terminal as claimed in any one of claims 3 to 10 configured for use in a system as claimed in claim 1 or 2.
12. A method of distributing content through a network to a terminal with a user interface to perform a plurality of individual user selectable operations for data content supplied to the terminal through the network, said operations being controlled in dependence on the data content **characterised by**

assigning and including indicia data in data content to be supplied through the network to the terminal, the indicia data indicating which of the plurality of individual user selectable operations are permitted for the data content by user selection at the terminal,

and controlling operation of the user interface of the terminal for the data content by the indicia data included therein such that said user selectable operations are each individually enabled or disabled in dependence on the indicia data.

13. A method of receiving data content through a network at a terminal comprising a user interface to perform a plurality of individual user selectable operations for the data content and said operations being controlled in dependence on the data content **characterised by**

receiving data content that includes indicia data indicating which of the plurality of individual user selectable operations are permitted for the data content by user selection at the terminal, and

controlling the operation of the user interface for the data content in dependence on the indicia data included therein such that said user selectable operations are each individually enabled or disabled in dependence on the indicia data.

14. A method as claimed in claim 13 wherein said user selectable operations include transferring the data content from a volatile memory of said terminal to a non-volatile memory of said terminal.

15. A computer program comprising executable code to perform a method as claimed in any one of the claims 12 to 14.