Title: SYSTEM AND METHOD FOR ADAPTING AN INTERNET AND INTRANET FILTERING SYSTEM

Abstract: According to the present invention, there is provided a system and method for continuously interfacing with a plurality of computer-based event monitoring systems such as Internet and Intranet filtering systems and or virus scanning software to determine whether these systems have detected a non-threatening and or security threatening event that corresponds with an event pre-determined and recorded within the events list which contains a plurality of non-threatening and security threatening events that may occur within a computer which in turn triggers a classified, targeted and value-adding hypertext message or information to be instantly displayed to the computer user through a browser or user interface instead of an event monitoring system default hypertext security message, and preferably an editing function shall be provided that enables the login of authorised authors including computer administrator(s) to edit and publish targeted and value-adding hypertext messages and information, and preferably a measuring function shall be provided that enables the login of authorised authors including computer administrator(s) to define and set up a plurality of metrics that may enable them to measure the effectiveness of the displayed targeted and value-adding hypertext messages and information in terms of being useful, entertaining, educational, interesting or instructional to a computer user through an alternate browser or user interface at the unique point in time when their computer has detected an event.
System and Method for Adapting an Internet and Intranet Filtering System

Field of the Invention

The present invention relates to a system and method for improved value utilisation and communication of Internet or Intranet page content using an Internet or Intranet browser or user interface with a domain name entry, Uniform Resource Locator (URL) and Internet or Intranet page content filtering system or other event monitoring system. In particular, the invention takes advantage of the interface to a content filtering system or other event monitoring system that filters prohibited domain name entries, URLs and Internet or Intranet page content or other events and diverts a user when they have deliberately or inadvertently caused a Internet or Intranet browser or other security threat or breach to provide to an improved viewing and reading experience for the user and a more effective, targeted and measurable delivery of communication for authorised authors.

Background to the Invention

The Internet is a global system of computers that are linked together so that the various computers can communicate seamlessly with one another. Internet users access server computers to download and display informational or hypertext pages typically through an Internet browser. Once a server has been connected to the Internet, informational or hypertext pages can be displayed to virtually anyone having access to the Internet. Alternatively, an Intranet is a private computer network that uses the protocols of the Internet but host informational or hypertext pages that can only be seen by a select number of network connected computers using an Intranet browser and hence a limited number of users.

Currently, documents available on the Internet are usually represented in the format of "hypertext." Each hypertext "page" can be arbitrarily long, and may or may not fit within one computer monitor screen. Pages of hypertext maybe linked to each other by "hyperlinks" on each page of a hypertext, and there might be one or more "links" in the form of static or animates pictures, video, words or embedded documents which, when selected and clicked on (with, say, an input device such as a
(computer mouse) will cause the hypertext document to which the hyperlink is linked to appear on the computer monitor screen. In other words, the text of the new page replaces the earlier hypertext page.

Domain name entry, Uniform Resource Locator (URL) and Internet or Intranet page content filtering systems interfaced with Internet or Intranet browsers are used to provide security and reduce threats such as prohibited domain names or URLs, undesirable emails, pop-ups, downloads and prohibited Internet or Intranet page content that may be categorised by the amount and type of language, nudity, sex or violence contained within a page. Other event monitoring systems that also detect undesirable or prohibited activities such as virus scanning software may be installed on a computer to provide additional security and reduce threats such as computer viruses, malware, spam, and phishing.

Typically content filtering systems or other 'watch dog' monitoring systems such as virus scanning software installed on a computer are event based, so when their predefined criteria or rules for detecting a potential security threat or breach are met, they are triggered to perform a series of procedures so as to protect a computer, network or user. For example, if a prohibited domain name, URL or prohibited Internet or Intranet page content is searched, selected or requested using a browser or hyperlink, then typically a filtering system would trigger a procedure that stops the request from linking to the prohibited domain name, URL or prohibited Internet or Intranet page content and hence stop the Internet or Intranet browser from displaying the prohibited domain name, URL or Internet or Intranet page content and instead display a Internet or Intranet page with a static default standard hypertext security message within the browser for the user to view and read detailing that a potential threat had been detected and thwarted, for example a security message may say "Access Denied". This standard security notification message typically remains displayed until the user decides to visit another domain name, URL, hyperlink to another Internet or Intranet page or close the browser. Once all triggered procedures are completed and the computer or network is no longer under security threat or breach, these filtering systems or other event monitoring systems such as virus scanning software continue to operate in the background of a computer and or network waiting to detect the next security threat or breach.
While the current function of Internet or Intranet browser filtering systems or other event monitoring systems such as virus scanning software affords users protection from threats, their static standard security notification message displayed on a hypertext page through a browser typically only detail in a few words that security has been breached and little else, which under-utilises the opportunity and potential to provide and communicate value-adding information back to the user at a point in time when they have deliberately or inadvertently caused an Internet or Intranet browser security threat or breach. The default standard hypertext security message provides basic and minimal information, and hence minimal usefulness and experience for the user. Further, conventional filtering systems or other event monitoring systems such as virus scanning software do not provide a function to enable authorised authors to edit in a live environment the typical default standard hypertext security message to communicate more effective and targeted value-adding information to the browser user that may be classified as useful, entertaining, educational, interesting or instructional at a unique point in time. Typically, once a filtering system or other event monitoring system such as virus scanning software displays its default standard hypertext security message within a browser or user interface it has completed its procedure and provides no further use or value to a user.

It is an object of this invention to overcome or substantially ameliorate the disadvantages of the prior art by providing a system and method that interfaces with a domain name, URL, Internet or Intranet page content filtering system and or other event monitoring systems such as virus scanning software which requires secure login by authorised authors at all times and enables users to edit and publish a hypertext security message/s in a live environment to communicate more effective, targeted and measurable information that may be classified as useful, entertaining, educational, interesting or instructional to a user through a browser or user interface at a point in time when they have deliberately or inadvertently caused a Internet or Intranet browser security threat or breach or when their computer's virus scanning software has detected a security threat to provide them an improved viewing and reading experience.
Summary of Invention

The system and method has several features, no single one of which is solely responsible for its desirable attributes. Without limiting the scope as expressed by what follows, its more prominent features will now be discussed briefly. After considering this discussion, and particularly after reading the section entitled "Detailed Description of the Invention" one will understand how the features of the system and method provide several advantages over conventional filtering systems and other event monitoring systems such as virus scanning software.

The present invention addresses the limitations in the conventional Internet or Intranet browser with a domain name entry, Uniform Resource Locator (URL) and Internet or Intranet page content filtering system and or other event monitoring systems such as virus scanning software by providing an interface system and method that enables authorised authors to communicate targeted and value-adding information to the user through a browser or user interface at the unique point in time when they have deliberately or inadvertently caused an Internet or Intranet browser security threat or breach or when their computer's virus scanning software has detected a security threat or breach, and improves utilisation of Internet or Intranet page content at this point in time which may be measured for its effectiveness as communicated information. Advantageously, this invention allows the communication of value-adding information to also be displayed to a user in the event that their computer has timed-out as an alternative to a standard computer monitor screen-saver.

The invention is installed on a standalone or networked computer and may comprise an events list which is either a local or centrally stored file on the computer that may contain a listing of possible non-threats such as a computer timing out, security threats such as computer viruses, malware and spam and or Internet or Intranet page identifiers, which typically are Uniform Resource Locators (URLs) and a content category related to allow-block lists used in a filtering system and the content category for each such Internet or Intranet page. A content settings function is further provided containing settings for the user as determined by the computer administrator. Such content settings may include an age group map that cross-references age groups to the categories of landing page permissibly and suggestibly viewable by the respective age group or their personal interests. Content settings may also include the user's interest-matching list, the user's age group and other
demographic based grouping as determined and customised by the administrator. Preferably authorised authors may access the events list and content settings by unique and secure password to classify and compile a plurality of different types of non-threatening and security threatening events that may occur within a computer, an Internet or Intranet filtering system or other area of a computer, for example a detectable threat or breach found by an installed virus scanning software, or a non-threatening event such as when a computer has timed-out, or a prohibited content is requested and is programmed to automatically display a standard notification or computer monitor screen-saver.

Preferably the invention continually interfaces with a plurality of computer based event monitoring systems such as filtering systems and or virus scanning software to determine whether these systems have detected a non-threatening event and or security threat or breach that corresponds with those detailed within the events list and content settings. Preferably when an event such as a security threat has been detected by an event monitoring system such as a filtering systems and or virus scanning software that corresponds to an event recorded on the events list, a corresponding tailored and targeted hypertext message and information is instantly displayed to the computer user through a browser or user interface by the invention.

Preferably an editing function shall be provided that enables the login of authorised authors including computer administrator/s by unique and secure password to edit and publish tailored and targeted hypertext messages and information that may be classified as useful, entertaining, educational, interesting or instructional to a computer user through a browser or user interface in the instant their computer's event monitoring systems detect an event corresponding to that recorded on the events list.

Preferably a measuring function shall be provided that enables the login of authorised authors including computer administrator/s by unique and secure password to define and set up a plurality of metrics that may enable them to measure the effectiveness of the published and communicated messages and information recorded within the editing function in terms of being useful, entertaining, educational, interesting or instructional to a computer user.
Additional advantages and the novel features of the invention will be set forth in the description which follows, and in part will be apparent to those skilled in the art upon examination of the following, or may be learned by practice of the invention.

Brief Description of Drawings

The present invention is described in detail below with reference to the attached drawing figure, wherein:

FIG. 1 is an illustration detailing an overview of the present invention.

Detailed Description of the Invention

The invention provides a system and method for continuously interfacing with a plurality of computer based event monitoring systems 1 such as Internet and Intranet filtering systems 2 and or virus scanning software 3 to determine whether these systems have detected a non-threatening and or security threatening event that corresponds with an event pre-determined and recorded within the events list 4 which contains a plurality of non-threatening and security threatening events that may occur within a computer 5 which in turn triggers a classified, targeted and value-adding hypertext message or information 6 to be instantly displayed to the computer user through a browser or user interface 7 instead of an event monitoring system 1 default hypertext security message, and preferably an editing function 8 shall be provided that enables the login of authorised authors 9 including computer administrator/s 10 to edit and publish targeted and value-adding hypertext messages and information 6, and preferably a measuring function 11 shall be provided that enables the login of authorised authors 9 including computer administrator/s 10 to define and set up a plurality of metrics 12 that may enable them to measure the effectiveness of the displayed targeted and value-adding hypertext messages and information 6 in terms of being useful, entertaining, educational, interesting or instructional to a computer user through a browser or user interface 7 at the unique point in time when their computer has detected an event.
The invention is preferably installed on a standalone or networked computer 13, with an events list 4, hypertext message list 14. Moreover, those skilled in the art will appreciate that the invention may be practised with other computer system configurations, including hand-held devices.

The events list 4 is preferably a listing of a plurality of non-threatening and security threatening events that may occur and be detected by computer base monitoring systems 1 such as Internet and Intranet filtering systems 2 and or virus scanning software 3 within a computer which is preferably accessible by unique and secure password to enable the login of authorised authors 9 including computer administrator/s 10 to edit and group these events by type such that hypertext messages and information 6 recorded on the hypertext message list 14 can be subsequently classified and subsequently displayed in the instant a particular event occurs. The present embodiment may operate with a pre-populated events list 4 to provide an authorised author 9 or administrator/s 10 a listing of typical events to choose from to save time.

Preferably this system and method continuously interfaces and communicates with a predetermined group of computer based event monitoring systems 1 such as Internet and Intranet filtering systems 2, virus scanning software 3 and standard computer alerts until it determines that a system/s or alert has detected a non-threatening and or security threatening event that corresponds with a predetermined event recorded within the events list 4. On installation of the system and method the installer shall be provided the option to search, select and pre-determine which computer based event monitoring systems 1 are to be continuously interfaced with. Preferably this system and method interfaces directly with that function of an event monitoring system 1 that stops or produces an event which subsequently displays a related default hypertext message, such as "Access Denied" or similar, and replaces this default message with a classified hypertext messages or information 6 from the hypertext message list 14 which is instead displayed to the user through a browser or user interface 7.

Preferably the system and method shall be provided an editing function 8 accessible by unique and secure password to enable the login of authorised authors 9 including computer administrator/s 10 to edit in a live environment hypertext messages and information 6 that may be defined as useful, entertaining, educational, interesting or instructional to a user through a browser or user interface 7,
and classify such messages and information 6 according to a plurality of predefined events and or content categories maintained on the events list 4 such that the hypertext messages and information 6 is targeted and displayed to the computer user through a browser or user interface 7 in the instant their computer's event monitoring systems 1 detect an event corresponding to that recorded on the events list 4, and maintain these hypertext messages and information 6 on the hypertext message list 14. For example, the age group for a primary school and the school's prohibited content categories may include pornography and gambling so that when a primary school child user attempts to access Internet or Intranet pages that may contain these prohibited categories the computer's filtering system's 2 detects the security threat and instead of this filtering system simultaneously displaying its standard default hypertext message of "Access Denied" or similar the invention by referencing the pre-determined events and content categories recorded within the events list 4 determines what type of event has occurred and selects a corresponding value-adding hypertext message 6 that may be entertaining, educational, interesting or instructional and displays this to the child user through a browser or user interface 7 to provide them an improved viewing and reading experience.

Preferably the system and method shall be provided a measuring function 11 which enables the login of authors 9 and computer administrator 10 who are authorised by unique and secure password to define and set up a plurality of metrics 12 that may enable them to measure the effectiveness of their displayed and communicated tailored, targeted and value-adding hypertext message and information 6 in achieving a desired level of effectiveness in terms of being useful, entertaining, educational, interesting or instructional to a computer user in the instant their computer's event monitoring system/s 1 detect an event corresponding to that recorded on the events list 4. A metric may be a static and or dynamic statistic that is set up, calculated via an algorithm and recorded within the measuring function 11 with the measured results collected and saved within the measuring function 11 every time a targeted and value-adding hypertext message and information 6 is displayed to a computer user, which may preferably be presented in a report 15 format within the measuring function 11 or extracted out of the measuring function 11 into another format to enable the authorised author 9 or administrator 10 to easily assess whether their hypertext message and information 6 has been viewed and or interacted with by the computer user the way they intended. For example, an author 9 of a targeted hypertext message 6 may be interested to measure whether a computer user is interacting with this message's hyperlinks and or in measuring how long in time
the user stays interacting within the displayed message 6 and or may survey users online on a number of specific questions to gauge their opinion on a particular subject/s. If the measured metric indicates that a displayed hypertext message or information 6 was effective in interacting with a computer user in the way they intended, then the authorised author 9 or administrator 10 may leave this information unchanged, or if the report 15 for a metric 12 indicates that a displayed hypertext message or information 6 was ineffective, then the authorised author 9 or administrator 10 may modify or delete the targeted hypertext information 6.

Although many other internal components of the computer are not detailed, those of ordinary skill in the art will appreciate that such components and the interconnection are well known. Accordingly, additional details concerning the internal construction of the computer need not be disclosed in connection with the present invention.

Finally, it is to be understood that the inventive concept in any of its aspects can be incorporated in many different constructions so that the generality of the preceding description is not to be superseded by the particularity of the attached drawing/s. Various alterations, modifications and/or additions may be incorporated into the various constructions and arrangements of parts without departing from the spirit or ambit of the invention.
The claims defining the invention are as follows:

1. A method for continuously interfacing with a plurality of computer based event monitoring systems such as Internet and Intranet filtering systems and or virus scanning software to determine whether these systems have detected a non-threatening or threatening event, and displaying editable hypertext messages and information that can be measured on standalone or networked computers, comprising steps of:
   - searching, selecting and determining computer based event monitoring systems;
   - determining, editing and recording non-threatening or threatening events on the events list;
   - editing and recording of hypertext messages and information for display;
   - classifying said hypertext messages and information;
   - editing and recording metrics to measure the effectiveness of said hypertext messages and information;
   - detecting and classifying non-threatening or threatening events on said events list;
   - displaying classified said hypertext messages and information; and
   - measuring effectiveness of said hypertext messages and information.

2. The method according to claim 1, wherein said steps of searching, selecting and determining computer based event monitoring systems are performed by accessing a computer's installed programs and their identification.

3. The method according to claim 1, wherein said steps of editing and recording of hypertext messages and information are performed within the message list.

4. The method according to claim 1, wherein said step of classifying hypertext messages and information is performed by reference to non-threatening or threatening events and content categories on said events list.

5. The method according to claim 1, wherein said step of displaying classified said hypertext messages and information is performed by use of alternate Internet or Intranet browser or user interface.
6. The method according to claim 1, wherein said step of measuring effectiveness of said hypertext messages and information is performed by at least one metric.

7. A system for continuously interfacing with a plurality of computer based event monitoring systems such as Internet and Intranet filtering systems and or virus scanning software to determine whether these systems have detected a non-threatening or threatening event, and displaying editable hypertext messages and information that can be measured on standalone or networked computers, comprising:

- an events list;
- a message list;
- a browser or user interface;
- editing function;
- measuring function; and
- a requester configured to dynamically request a hypertext message or information from the message list to be instantly displayed in response to determined event on a computer.

8. A system for displaying a hypertext message and information into an alternate Internet and Intranet browser or user interface, comprising:

- a secure login function configured to enable an authorised author or computer administrator to login by unique and secure password in a live computer environment;
- a secure editing function configured to enable an author or computer administrator to edit and save a plurality of hypertext messages and information;
- a list of classifications to enable an author or computer administrator to classify a hypertext message and information corresponding to known non-threatening or threatening events, including prohibited content categories or particular user's age groups; and
- a request processor configured to dynamically receive a request from an event monitoring system for said hypertext message and information to be displayed in an alternate Internet or Intranet browser or user interface.

9. A system for measuring the effectiveness of hypertext messages and information when
displayed to a computer user through a browser or user interface, comprising:

- a secure login function configured to enable an authorised author or computer administrator to login by unique and secure password in a live computer environment;
- a secure editing function configured to enable an author or computer administrator to define, set up, edit and save a plurality of metrics;
- a content request function configured to dynamically collect and record data required for said metrics;
- an algorithm that calculates the difference between said metrics and said collected data; and
- a display mechanism configured to format said metrics, collected data and said differences for reporting to and viewing by an author or computer administrator.
1. A method for continuously interfacing with a plurality of computer based event monitoring systems such as Internet and Intranet filtering systems and or virus scanning software to determine whether these systems have detected a non-threatening or threatening event predetermined and recorded within an events list, and displaying editable hypertext messages and information corresponding to classification on a message list that can be measured on standalone or networked computers, comprising steps of:

- searching, selecting and determining computer based event monitoring systems;
- determining, editing and recording non-threatening or threatening events on the events list;
- editing and recording of hypertext messages and information for display on the message list;
- classifying said hypertext messages and information;
- editing and recording metrics to measure the effectiveness of said hypertext messages and information;
- detecting and classifying non-threatening or threatening events on said events list;
- displaying classified said hypertext messages and information; and
- measuring effectiveness of said hypertext messages and information.

2. The method according to claim 1, wherein said steps of searching, selecting and determining computer based event monitoring systems are performed by accessing a computer's installed programs and their identification.

3. The method according to claim 1, wherein said steps of editing and recording of hypertext messages and information are performed within the message list.

4. The method according to claim 1, wherein said step of classifying hypertext messages and information is performed by reference to non-threatening or threatening events and content categories on said events list.

5. The method according to claim 1, wherein said step of displaying classified said hypertext
messages and information is performed by use of alternate Internet or Intranet browser or user interface.

6. The method according to claim 1, wherein said step of measuring effectiveness of said hypertext messages and information is performed by at least one metric.

7. A system for continuously interfacing with a plurality of computer based event monitoring systems such as Internet and Intranet filtering systems and or virus scanning software to determine whether these systems have detected a non-threatening or threatening event predetermined and recorded within an events list, and displaying editable hypertext messages and information corresponding to classification on a message list that can be measured on standalone or networked computers, comprising:

- an events list;
- a message list;
- a browser or user interface;
- editing function;
- measuring function; and
- a requester configured to dynamically request a hypertext message or information from the message list to be instantly displayed in response to determined event on a computer.

8. A system for displaying a hypertext message and information into an alternate Internet and Intranet browser or user interface, comprising:

- a secure login function configured to enable an authorised author or computer administrator to login by unique and secure password in a live computer environment;
- a secure editing function configured to enable an author or computer administrator to edit and save a plurality of hypertext messages and information;
- a list of classifications to enable an author or computer administrator to classify a hypertext message and information corresponding to known non-threatening or threatening events, including prohibited content categories or particular user's age groups; and
- a request processor configured to dynamically receive a request from an event monitoring
system for said hypertext message and information to be displayed in an alternate Internet or Intranet browser or user interface.
STATEMENT UNDER ARTICLE 19 (1)

The amendments to claims were made to ensure all key aspects of the invention were detailed as clearly as possible. The amendments made to claims have no impact on what is described in the patent description or detailed in the drawing.
### INTERNATIONAL SEARCH REPORT

**A. CLASSIFICATION OF SUBJECT MATTER**

Int. Cl.

G06F 11/30 (2006.01)  
G06F 21/00 (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database consulted during the international search (name of database and, where practicable, search terms used)

EPDOC & WPI, Google, Google Scholar, Google Patents, USPTO, & Google Patents, USPTO, & Google Patents, USPTO, & Google Patents, USPTO.

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>US 661 5266 B1 (HOFFMAN, JR. et al) 02 September 2003 (see entire document)</td>
<td>1-9</td>
</tr>
<tr>
<td>A</td>
<td>US 5884033 (DUVALL et al) 16 March 1999 (see entire document)</td>
<td>1-9</td>
</tr>
</tbody>
</table>

* Further documents are listed in the continuation of Box C  
X See patent family annex

**Date of the actual completion of the international search**  
22 February 2010

**Date of mailing of the international search report**  
4 April 2010

Name and mailing address of the ISA/AU

AUSTRALIAN PATENT OFFICE  
PO BOX 200, WODEN ACT 2606, AUSTRALIA  
E-mail address, pct@ipaustralia.gov.au  
Facsimile No. +61 2 6283 7999

Authorized officer  
Andrew Munro

AUSTRALIAN PATENT OFFICE  
(ISO 9001 Quality Certified Service)  
Telephone No. +61 3 9935 9620.
### Box No. II  Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. **Claims Nos.:**
   - because they relate to subject matter not required to be searched by this Authority, namely:

2. **Claims Nos.**:
   - because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. **Claims Nos.**:
   - because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a)

### Box No. III  Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

See continuation of Box III.

1. **[X]** As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. **[ ]** As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. **[ ]** As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. **[ ]** No required additional search fees were timely paid by the applicant. Consequently, this International search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

### Remark on Protest

- **[ ]** The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

- **[ ]** The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

- **[X]** No protest accompanied the payment of additional search fees.

Form PCT/ISA/2 10 (continuation of first sheet (2)) (July 2008)
Supplemental Box
(To be used when the space in any of Boxes 1 to IV is not sufficient)

Continuation of Box No III:

This International Application does not comply with the requirements of unity of invention because it does not relate to one invention or to a group of inventions so linked as to form a single general inventive concept.

In assessing whether there is more than one invention claimed, I have given consideration to those features which can be considered to potentially distinguish the claimed combination of features from the prior art. Where different claims have different distinguishing features they define different inventions.

This International Searching Authority has found that there are different inventions as follows:

- Claims 1-8 are directed towards an event monitoring system to determine if they have detected non-threatening or threatening events and displaying hypertext messages corresponding to the detected events. It is considered that the detection of non-threatening or threatening events comprises a first distinguishing feature.

- Claim 9 is directed towards a method and system for measuring the effectiveness of hypertext messages and information when displayed to a computer user through a browser or user interface. It is considered that the measuring of the effectiveness of hypertext messages comprises a second distinguishing feature.

PCT Rule 13.2, first sentence, states that unity of invention is only fulfilled when there is a technical relationship among the claimed inventions involving one or more of the same or corresponding special technical features. PCT Rule 13.2, second sentence, defines a special technical feature as a feature which makes a contribution over the prior art.

Each of the abovementioned groups of claims has a different distinguishing feature and they do not share any feature which could satisfy the requirement for being a special technical feature. Because there is no common special technical feature it follows that there is no technical relationship between the identified inventions. Therefore the claims do not satisfy the requirement of unity of invention a priori.
This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>US 2007061459</td>
<td>US 2007058668</td>
</tr>
<tr>
<td>US 6615266</td>
<td>US 6122657</td>
</tr>
<tr>
<td>US 5884033</td>
<td>NONE</td>
</tr>
</tbody>
</table>

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX