Claim

1. A method for identifying software capable of capturing personally identifiable information from a local device, comprising the steps of:

connecting to a remote server via the local device in order to send at least one request for data and retrieve at least one packet of data in response to the request, wherein connecting to the remote server does not require access to the remote server by the local device;

determining whether the received requested data originated from a third party server other than the remote server, and if so, determining whether the received data contains evidence of the presence of personally identifiable information provided to the remote server by the local device.

2. A method in accordance with claim 1, wherein the step of determining whether the received data contains personally identifiable information includes the step of determining whether the received data includes data that has a specific signature pattern.

3. A method in accordance with claim 2, comprising the further step of determining whether the data has the specific signature pattern by comparing the data to a database of signature data patterns.

4. A method in accordance with claim 2 or claim 3, comprising the further step of sending data with the specific signature pattern to an identification module arranged to classify the data into data that contains personally identifiable information or into data that does not contain personally identifiable information.

5. A method in accordance with any one of claims 1 to 4, wherein the received data is sent to a user to allow the user to further classify the data, wherein the classification elected by the user is utilised to provide input to the identification module.

6. A system for identifying software capable of capturing personally identifiable information, the system comprising:

a module arranged to connect to a remote server via a local device and

an identification module;

wherein:

connecting to the remote server does not require access to the remote server by the local device;

the module is further arranged to send at least one request for data and retrieve at least one packet of data in response to the request; and

the identification module is arranged to:

receive the at least one requested packet of data, and

determine whether the received data originated from a third party server other than the remote server, and if so, to determine whether the received data contains evidence of the presence of personally identifiable information provided to the remote server by the local device.

7. A system in accordance with claim 6, wherein the identification module further includes a routine which determines whether the received data includes data that has a specific signature pattern.

8. A system in accordance with claim 7, wherein the identification module further includes a routine which determines whether the data has the specific signature pattern by comparing the data to a database of signature data patterns.

9. A system in accordance with claim 7 or claim 8, wherein the identification module sends data with the specific signature pattern to an identification module arranged to classify the data into data that contains personally identifiable information or into data that does not contain personally identifiable information.

10. A system in accordance with any one of claims 6 to 9, wherein the identification module sends the received data to a user to allow the user to classify the data, wherein the classification elected by the user is utilised as input to the identification module.

11. A computer program, including at least one instruction and arranged to be executable on a computing system, wherein, upon execution, the computing system performs the method of at least one of claims 1 to 5.

12. A data signal, including at least one encoded instruction and arranged to be received and executed on a computing system, wherein, upon receipt and execution, the computing system performs the method of at least one of claims 1 to 5.