

the parties while maintaining the anonymity of the parties and the requestor from each other. The invention, however, is not limited to those types of applications. Other applications include finding and interviewing consultants or freelancers for a specific project, auditioning actors and actresses, seeking a merger partner, and engaging in various commerce-based applications in which controlled anonymity by any party would be beneficial.

The invention can be used in applications where the system establishes a communications channel between parties and authenticates information about the parties, while maintaining the anonymity of at least one of the parties. In one embodiment, system **100**, as described above, could be used for such applications. This embodiment allows two parties to communicate while each party is ensured that the information being communicated is valid. For example, in the case of a “whistle-blowing” application (outlined below) an employer can be certain that the information he receives is from an employee within his organization. The methods illustrated by the flow diagrams of FIGS. **5–9** could be readily adapted for these applications.

By way of example, system **100** could be used as a “whistle-blowing” system to allow employees of a company to anonymously report legal and policy violations without risking retribution by the company’s management. The employee reporting a violation would preferably enter, into party terminal **300**, data about the violation and data that can be independently verified as originating from the employee claiming the violation. The employee is referred to hereafter as the “party” and the data entered into party terminal **300** is referred to hereafter as the “party data.” In one embodiment, the party data may include an employee identification number uniquely identifying each employee of the company. Party terminal **300** encrypts and transmits the party data to central controller **200**, preferably in the manner described above.

A company representative, referred to as the “requester,” would use requester terminal **400** to access the party data stored in central controller **200**. After accessing the party data about the violation, the requester could submit a request at requester terminal **400** to have some or all of the party data authenticated. For example, central controller **200** could verify that the party is, in fact, an employee of the company by comparing an employee identification number contained in the party data with a list of active company employee identification numbers. If the number matches, central controller **200** would transmit a response to requester terminal **400** confirming that the party is an active employee of the company.

The requester, or the party, could enter a request into requester terminal **400**, or party terminal **300**, for central controller **200** to open a communications channel with the party, or the requester. Central controller **200** would open a communications channel, as described above in connection with FIGS. **8** and **9**, to allow the party and the requester to communicate, while maintaining the party’s anonymity. This would allow the employer to question the employee about details relating to the incident in question, without the employee revealing his identity.

In another example, system **100** could be used as a system to allow parties to remain anonymous while negotiating an agreement. For instance, criminals, or rule offenders, anonymously offer to turn themselves in, while negotiating favorable treatment. In this case, the criminals, or rule offenders, would represent the “parties” and law enforcement, or rule enforcers, would represent the “requesters.” In a preferred embodiment, a party would enter, at party terminal **300**,

information (“party data”) about his violation and data that can be independently verified as originating from the party claiming the violation. The party data can include the party’s identity, which is preferably only used by system **100** for verification purposes. Party terminal **300** would encrypt and transmit the party data to central controller **200**, in the manner described above. A requester would use requester terminal **400** to access the party data stored in central controller **200**.

The requester could enter a request for authentication of the party data into requester terminal **300**, which would transmit the request to central controller **200**. Central controller **200** would verify some or all of the party data, as described above, and transmit a verification status message to requester terminal **400**. Upon request from either party terminal **300** or requester terminal **400**, central controller can establish an anonymous communications channel with the other terminal, provided that the party and the requester agree to engage in the communications channel. As described above, this communications channel can be real-time or non-real-time.

Under the “plea bargaining” example, the invention allows the requester and the party to negotiate the terms of the party’s sentence or punishment for committing the violation before the party reveals his identity. If negotiations fail, the party does not subject himself to any risk that the requester will learn his identity simply because he initiated communication. The requester, of course, can use whatever information the party revealed about himself during the course of the negotiation to learn the identity of the party.

Besides the whistle-blowing and plea bargaining examples, the invention also applies to other applications, such as authenticated phone-based tip lines and licensing negotiations where a licensee does not want to reveal the size of his company for fear of being charged more by the licensor.

Conclusion

It will be apparent to those skilled in the art that various modifications and variations can be made in the system and method of the present invention without departing from the spirit or scope of the invention. The present invention cover the modifications and variations of this invention provided they come within the scope of the appended claims and their equivalents.

What is claimed is:

1. A method for facilitating an exchange of information between a first party and a second party, comprising the steps of:

receiving first party information data from said first party; storing said first party information data in a secure database;

receiving, from said first party, at least one first party rule for releasing said first party information data;

storing said at least one first party rule;

receiving, from said second party, a search request to the secure database, said search request comprising at least one search criterion to be satisfied;

determining second party data relevant to said at least one first party rule;

receiving, from said second party, at least one second party rule for releasing said second party data;

processing said search request from said second party to determine if said first party information data satisfies said at least one search criterion;