December 2006

When the Public has a Right to Know: Using Toulmin's Method to Protect Sensitive Information on Government Websites

Abhijit Jain
Temple University

When the Public has a Right to Know: Using Toulmin's Method to Protect Sensitive Information on Government Websites

Abhijit Jain
Temple University and Northern Michigan University
jain@temple.edu

ABSTRACT

Publicly accessible U.S. government websites often provide sensitive information that can be abused by terrorists. For example they may provide extensive information on a region's nuclear power plants or water supply systems or emergency preparedness. It is possible for terrorists and other malcontents to use such information to identify 'soft targets'. However, due to laws such as the Freedom of Information Act, and also due to precedent, the government cannot simply choose not to provide much of this information. This calls for a mechanism whereby the government may be able to intelligently control the dissemination of information so as to reduce the probability of sensitive information falling into the wrong hands.

In particular, the government needs a system to analyze and assess the legitimacy of claims to information. This paper proposes an agent-based framework that has the potential to allow the government to control, in an intelligent fashion, the dissemination of sensitive information via government websites. This framework employs the 'Toulmin method for analyzing arguments' to assess the legitimacy of claims to information on government websites.

Keywords

Government Websites, Toulmin, Information Security.

INTRODUCTION

On January 17, 2002 the FBI alerted 18,000 law enforcement bodies in the U.S. that suspected Al Qaeda terrorists had been looking at websites of U.S. nuclear power plants prior to 9-11 (Watson and Kay, 2002). Not only did this give rise to an immediate concern (i.e. were terrorists targeting nuclear plants next?), but it also underscored a much deeper, long term concern - the potential for abuse of a large amount of information that the U.S. government provides to the public freely, and is required to provide by law.

The issue is complex. The Freedom of Information Act (1966, with major amendments in 1974 and 1996) requires the U.S. government to provide the public with a vast amount of information. Synchronistically, the Paperwork Reduction Act (1995) requires the U.S. government to move a vast quantity of information online and follow a time-schedule in doing so. In addition to information on how it makes decisions or how it spends taxpayer money, the government has traditionally provided the American public all manner of other information including extensive details on public infrastructure such as roads, bridges, waterways, power grids, power plants and nuclear and military installations. Further, it has also provided wide-ranging information on government and military personnel.

Once upon a time, the provision of most such information was considered innocuous and harmless. However, times have changed, and today it is widely recognized that such information could be used by terrorists to find out about so-called potential soft targets; i.e. potential targets that are not adequately protected or that could lead to a large amount of damage. It is not difficult to imagine scenarios where terrorists or other malcontents may try to poison a major water system, or target a nuclear plant close to a densely populated residential area, or try to kidnap the security chief of a nuclear power plant to gain access to the plant, etc.

The government thus faces a dilemma. It is required by law to provide the public with information that can be used to bring harm to the public and to the government. Recognizing such possibilities in the aftermath of 9-11, the government reacted by either removing a vast quantity of information from the websites of various agency websites or by shutting down entire websites altogether. For example, the website of the Nuclear Regulatory Commission (www.nrc.gov), which used to provide

extensive information on all the nuclear power plants in the U.S., was completely shut down on October 11, 2001; one month after 9-11; and some people complained that this was still too late, that it should have been shut down immediately after 9-11 (Bivens, 2001). Though the website is back up now, it currently offers only threadbare information. Similarly, as described in the next section, a large number of other U.S. government websites too have undergone a similar course of action.

For the U.S. government, however, such withdrawal of information comes with its own set of problems. As has already been mentioned, the Freedom of Information Act requires the government to make most such information available to the American public; and the USA has a tradition of government transparency and openness. While the public, the press and groups such as the ACLU (American Civil Liberties Union) and Electronic Frontier Foundation may excuse the government for tightly controlling information in the short run (due to contemporary exigencies of the ongoing war against terrorism), they will expect the government to revert back to business as usual (i.e. providing information freely as was done before 9-11) in the long run; and will raise a hue and cry if the government does not do so.

In such a situation, what can the government do so as to fulfill its constitutional obligations (i.e. provide information to the public) and yet control the dissemination of sensitive information so as to reduce the probability of terrorists and other malcontents getting their hands on such information?

The obvious solution for the government would be to carefully control the dissemination of sensitive information. By keeping close tabs on who is requesting sensitive information and for what reason, the government can reduce the probability of sensitive information falling into the wrong hands (such a process still will not eliminate the *possibility* of such information falling into the hands of terrorists, but it would be fair to argue that complete elimination of such risk is practically impossible).

This paper proposes a framework that can allow the government to provide sensitive information electronically via government websites, albeit in an intelligently controlled fashion.

This paper is organized in the following way. In the next section, the problem of sensitive information on government websites is discussed in greater detail. The subsequent section provides a discussion of the concept of software 'agents'. In the section after that, the Toulmin method for analyzing claims is explained with an example. In next, the penultimate section, a framework for protecting sensitive information on government websites is described. The concluding section discusses limitations of the the framework along with directions for future research.

THE PROBLEM OF SENSITIVE INFORMATION ON GOVERNMENT WEBSITES

After the events of 9-11, not surprisingly, the U.S. government grew increasingly concerned about the vulnerability of the information available on the websites of its many agencies. A vast quantity of information, such as information on public infrastructure or emergency preparedness is vulnerable to being abused by potential terrorists who can put two and two together and spot soft targets; for example an inadequately guarded nuclear power plant that may be located near a large city or a city that is poorly prepared for a terrorist attack.

The U.S. government responded to such concerns by either removing vast quantities of information from its websites, or by shutting down entire websites altogether. The Electronic Frontier Foundation (2003) provides a detailed listing of such actions. A partial listing of such actions is provided below and makes for intriguing and insightful reading (from the Electronic Frontier Foundation website):

U.S. Government websites that shut down or removed information:

(All from Electronic Frontier Foundation, 2003)

> **Agency for Toxic Substances and Disease Registry**
>
> OMB Watch, a Washington group that advocates for government accountability in budgetary and regulatory matters, says the Agency for Toxic Substances and Disease Registry dropped a report critical of chemical plant security.
>
> **Centers for Disease Control and Prevention**
>
> OMB Watch, a Washington group that advocates for government accountability in budgetary and regulatory matters, says the Centers for Disease Control and Prevention has pulled a report about lack of preparedness against a terrorist attack using poison gas or other chemical agents.

Department of Energy, National Transportation of Radioactive Materials

The Department of Energy, National Transportation of Radioactive Materials site has been replaced with the note This site temporarily unavailable, Please contact Bobby Sanchez at 505-845-5541 if you have any questions, OMB Watch.

Environmental Protection Agency

OMB Watch, a Washington group that advocates for government accountability in budgetary and regulatory matters, says the EPA has pulled from its site Risk Management Plans, which contain detailed information about the dangers of chemical accidents -- such as toxic plume maps and emergency response plans after a refinery explosion.

Federal Aviation Administration

OMB Watch, a Washington group that advocates for government accountability in budgetary and regulatory matters, says the Federal Aviation Administration has pulled data from a site listing enforcement violations such as weaknesses in airport security.

Federal Energy Regulatory Commission

The Federal Energy Regulatory Commission, has removed documents that detail specifications for energy facilities from its website.

International Nuclear Safety Center

Selecting the Reactor Maps link from the front page of this site generates the following message: If you requested access to the maps of nuclear power reactor locations, these maps have been taken off-line temporarily pending the outcome of a policy review by the US Department of Energy and Argonne National Laboratory, while their Power Reactors database still lists city and state for nuclear plants around the world.

Los Alamos National Laboratory

The Los Alamos National Laboratory has removed a number of reports from its Laboratory Publications page, OMB Watch.

NASA Glenn Research Center

The NASA Glenn Research Center website notes that Public access to many of our web sites is temporarily limited. We apologize for any inconvenience, OMB Watch.

Nuclear Regulatory Commission

The Nuclear Regulatory Commission is displaying only only select content while performing a review of all material on their website, although most of the information has been there for years and nothing top secret was on the Web site to begin with.

U.S. Geological Survey

The U.S. Geological Survey has removed a number of pages from its Registered Online Water-Resources Reports database (search for removed), OMB Watch.

These actions (i.e. removing information from government websites or shutting down government websites) may be considered justifiable in the short term, considering the fact that the U.S. was only recently attacked and is currently at war with terrorists. However, in the long term, the government may be forced to adopt a different strategy. This is because of two reasons. Firstly, the Freedom of Information Act makes it mandatory for the government to freely provide, to the American public, a vast quantity of information held by government agencies. In fact, most information that is contained within the government is required to be released on a periodic basis. The only information that the government can hold back is that which has a very high probability of compromising the security of the country. And even in the case of such compromising information, most such information is required to be made public within a certain number of years (usually 25 years). Only a constitutional amendment can change these requirements and so far there has been no indication that such a path may be

followed. Secondly, the U.S. has a very strong institution of press freedom. The press will fight any government attempt to scale back the information it provides to the public (and judging by the frequent leaks to the press on plans related to the recent war in Iraq, it seems it is nearly impossible for the U.S. government to shield even top-secret information from the press). Thus, the press is not likely to take kindly to the idea of the government being secretive with information if this situation carries on for too long. Unless the U.S. government wants a long and hard fight with the country's press, it will eventually have to be more forthcoming with the information it is constitutionally required to furnish. Watershed historical events such as the Watergate scandal, the Iran-Contra affair and the Lewinsky affair serve to remind us that the government has little hope of winning an out and out battle against the press.

Therefore, the government needs a system to analyze and assess the legitimacy of claims to information. In the following sections, an agent-based framework is proposed, that has the potential to allow the government to control, in an intelligent fashion, the dissemination of sensitive information via government websites. This framework employs the 'Toulmin method for analyzing arguments' to assess the legitimacy of claims to information on government websites.

AN OVERVIEW OF AGENTS

There is no universal definition of a 'software agent' (Desharnais et al., 2002). However, a widely accepted notion of software agents has been provided by Wooldridge and Jennings (1995, 1999). According to them, 1) a software agent is a software object that pursues predetermined objectives defined by a user (a user may be a human agent or another software agent); 2) software agents function in particular environments that are usually co-habited by other agents and processes; and 3) software agents typically exhibit the following properties:

a) Autonomy: Agents have the capability to exert non-trivial control over their internal state and behavior. They are not necessarily invoked by a user (users can be humans or other agents), do not require explicit permission for every action, and can perform tasks without direct intervention from users.

b) Social Ability: Agents interact and collaborate with other agents via a communication language. In addition to pursuing their own objectives, agents may also help other agents with their objectives.

c) Reactivity: Agents can perceive their environment and can react to changes in the environment.

d) Proactivity: Agents are proactive. They can take the initiative and create goals proactively.

Additionally, according to Wooldridge and Jennings, so called intelligent agents exhibit the following properties:

e) Mobility: Intelligent agents are endowed with the ability move around electronic networks and carry out delegated tasks.

f) Veracity: Intelligent agents do not communicate false information knowingly.

g) Rationality: Intelligent agents do not knowingly act in ways that are detrimental to the achievement of their goals, at least insofar as their beliefs permit.

Thus, in a sense, software agents may be deemed to possess certain human-like capabilities and may be used to substitute for human agency in a limited way.

In recent years, agents have become grown up in scientific terms (Petta and Muller, 2000), agent technology seems to be well on its way into commercialization (ibid), and agents are able to solve real problems in certain domains (ibid). According to Petta and Muller, Information services (AskJeeves) and web portals (Go2Net), toys and entertainment products (Furbies, Lego robots) are recent examples of commercial products that employ various aspects of agent technology.

Agents have been used to support research in a variety of contexts. For example, agent based research has been used to:

- model emergent phenomena such as the collective behavior of people in crowds, markets and organizations (cf. Bonabeau, 2002).
- help in scanning the competitive environment (cf. Liu, 1998).
- help in searching for the best prices (cf. Kephart and Greenwald, 2000).
- model end-user support to computer users (cf. Desharnais et al., 2002)
- model decision support systems (cf. Aliev et al., 2000)
- model electronic marketplaces (cf. Padovan et al., 2002)

- model legal argumentation (cf. Stranieri and Zeleznikow, 2001)
- model provision of E-Government services (cf. Fernandes et al., 2001)

Despite their limited intelligence compared to humans, agents can sometimes perform 'intelligent' tasks more efficiently than humans. For example, the quantity and volatility of data on the internet can intimidate a human who needs to search through internet data, but agents can be used quite effectively to search such data (cf. March et al., 2000).

THE TOULMIN METHOD TO ANALYZE CLAIMS

The Toulmin method (Toulmin, 1958) is a technique to analyze the logic of an argument. This widely used technique estimates the worth of a claim by analyzing the argument that motivates the claim. By analyzing the argument behind a claim in this way, one can determine whether or not the claim should be considered valid.

According to Toulmin, an argument consists of six components. These six components are:

1. The Claim
2. The Data
3. The Warrant
4. The Backing (for the Warrant)
5. The Qualifier
6. The Rebuttal

Diagrammatically, the layout for the six components of an argument can be represented as in figure 1:

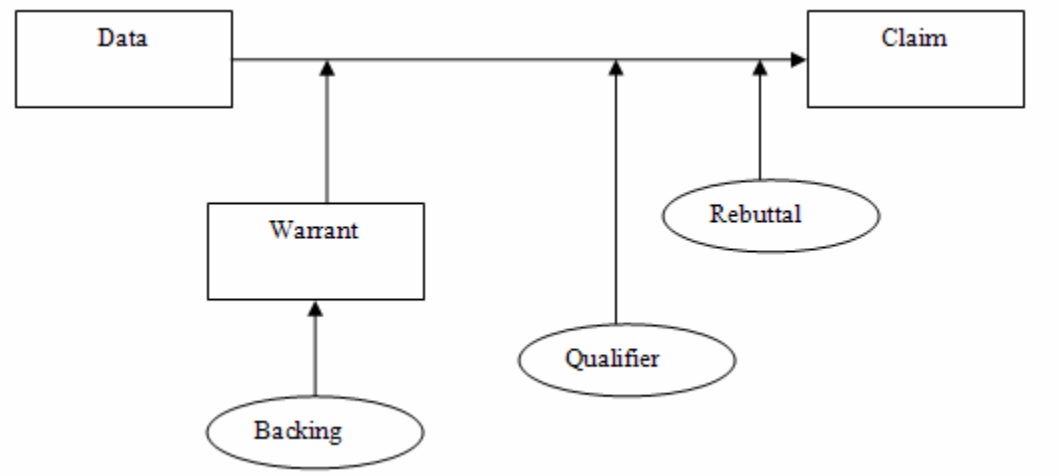

Fig. 1: The Toulmin Method

An example will now be used to explain this layout and each of these components. Consider the case of a university library. Let's say that only university faculty, students and staff are allowed to enter this library. Now consider a scenario wherein a person arrives at the library gates and claims that she should be allowed entry to the library because she is a student. The Toulmin method would analyze the person's argument (that she should be allowed entry to the library) in the following manner:

1. Claim: *The person should be given permission to enter the library.*

   The claim is the part of the argument whose validity has to be tested.

2. Data: *The person has student ID card.*

   The data provides the evidence for the claim.

3. Warrant: *Persons with student ID cards are students.*

   The warrant explains why the data should be considered evidence for the claim.

4. Backing: *Only student are issued student ID cards.*

   The backing provides support for the warrant, usually via theoretical or empirical reasoning.

5. Qualifier: *The person is 'probably' a student.*

   The qualifier anticipates the rebuttal of the argument and provides a measure of how strong the claim is or should be.

6. Rebuttal: *It is possible to create a fake student ID card.*

   The rebuttal illustrates possible reservations about the claim or rebuttals against it.

Although it seems deceptively simple, the Toulmin method has proved to be a powerful method for assessing the validity of claims. If the data, warrant or backing components are weak, the claim stands on shaky ground. Further, if the qualifier or rebuttal is too strong, then too the claim stands on shaky ground.

In recent years, the Toulmin method has been used to analyze discourses and to assess claims in many disciplinary contexts. For instance, the Toulmin method has been used in the fields of *Communication* (Bozik, 1984; Farmer, 1998; Johnson, 1995; Lunsford, 2002; Moag, 1966.Schultz and Germeroth, 1998), *Education* (Jimenez-Aleixandre, 2002; Jimez-Aleixandre and Rodriguez, 2000; Novak, 1979; Stephan and Rasmussen, 2002; Whitenack and Knipping, 2002; Young, 2000), *Linguistics* (Trent, 1968), *Management* (Gold et al., 2002), *Law* (Alison et al., 2003; Stranieri, 2002; Stranieri et al., 2000, Winters, 1998), *Urban Planning* (Gasper and George, 1998; Teller, 2001), *Consumer Behavior* (Boller et al., 1990), *Philosophy* (Allegretti and Frederick, 1995; Beck and Denis, 1993, Braunack-Mayer, 2001; Chambers, 2000; Hicks, 1998; Roberts, 1996; Wenz, 1997), *Rhetoric* (Chambliss, 1995; Janssen and Sage, 2000), *Medicine* (Horton, 1998); *Theology* (Keenan, 1993) and *Public Policy* (Locks, 1985).

The Toulmin method has also found favor in IS (information systems) research; for example, it has been used to inform research in *E-Democracy* (McBurney and Parsons, 2001), *Group Decision Support Systems* (Janssen and Sage, 2000) and *Knowledge Management* (Gregor, 1999).

In the next section, an agent-based framework for protecting sensitive information on government websites is developed using concepts from the Toulmin method.

A PROPOSED FRAMEWORK TO ANALYZE CLAIMS TO INFORMATION

This framework uses the Toulmin method to analyze the validity of claims for access to information in government websites.

The framework works in the following way: A user (customer) of a government website requests access to (i.e. makes a claim to) information on the website. If the claim is found valid, then the customer is provided online access to the requested information. If, however, the claim is found invalid or not valid enough, then the customer may be refused online access to the requested information. In the case that a customer is refused online access to requested information, there are two possible outcomes that can ensue. In certain cases, instead of online access to the information, the government may agree to give offline access to the same information in the manner described in section 2 (i.e. via physical archives that have to be personally visited). The government may adopt this route in cases where it is required to divulge certain information to the public by law (e.g. by the Freedom of Information Act) but is not comfortable giving it '*online'* to the said customer. This scenario allows the government to fulfill its constitutional obligations, and also closely monitor the requesting customer when the customer visits a physical archive to obtain the requested information. On the other hand, in certain cases, the government may choose to completely refuse the requested information to the said customer, whether via online or offline means, citing adequate justifications (the Freedom of Information Act allows the government to hold back information under certain conditions – e.g. if the information is certain to compromise national security).

According to this framework, there exist up to four layers of agents between the user (customer) of a government website and the information that the user seeks from the government website. The framework is visually represented in figure 2 and works in the following way. When a user (customer) of a government website (such as the website of the Nuclear Regulatory Commission) makes a request for information, the request is first sent to a layer of agents called the 'Information Request Diagnostic Layer'. This layer contains a software agent called 'Claim Agent'. The 'Claim Agent' parses through the customer's request, breaking the request into specific claims for information, and forwarding these claims to the 'Decision Layer'.

The 'Decision Layer' contains software agents called 'Warrrant Agent', 'Backing Agent', 'Qualifier Agent', 'Rebuttal Agent' and 'Verdict Agent'. When a claim from the 'Information Request Diagnostic Layer' reaches the 'Decision Layer', the 'Warrant Agent' in the 'Decision Layer' consults with the 'Backing Agent' to determine whether the claim can be honored 'as is' (the claim is honored 'as is' if the information being sought is not *sensitive*). The 'Backing Agent' has access to databases of claims and decision rules that allow it advise the 'Warrant Agent' on whether the claim is valid (i.e. whether it may be honored 'as is'). The 'Qualifier Agent' and 'Rebuttal Agent', which also have access to relevant databases of claims and decision rules, lend further nuance to the Backing Agent's assessment. The 'Qualifier Agent' assigns a probability to the Backing Agent's assessment (i.e. probability that the information being requested is or is not sensitive). The 'Rebuttal Agent' rebuts the assessment of the 'Backing Agent' by furnishing an estimate of possible reservations (if any) against the Backing Agent's assessment. The 'Verdict Agent' judges the overall validity of the claim by weighing the assessments from the Warrant, Backing, Qualifier and Rebuttal Agents. If the claim does not raise a red flag, then the 'Verdict Agent' allows the claim to proceed to the 'Government Information Resource'; i.e. the request (i.e. claim to) information is honored and the information is provided online. If the claim raises a red flag for some reason (e.g. the information being sought is sensitive) then the 'Verdict Agent' requests the 'Warrant Agent' in the 'Decision Layer' to collect additional data regarding 'who' is making the claim.

The 'Warrant Agent' then queries the 'Client Authorization Diagnostic Layer' for information on the customer's identity. The 'Client Authorization Diagnostic Layer' contains a software agent called 'Data Agent' which then finds out more information about the customer who is requesting the information. This is done by furnishing the customer with a form on which personal identifying data is required to be entered by the customer (the lines to depict this interaction have not been shown in figure 2 in order to reduce clutter).

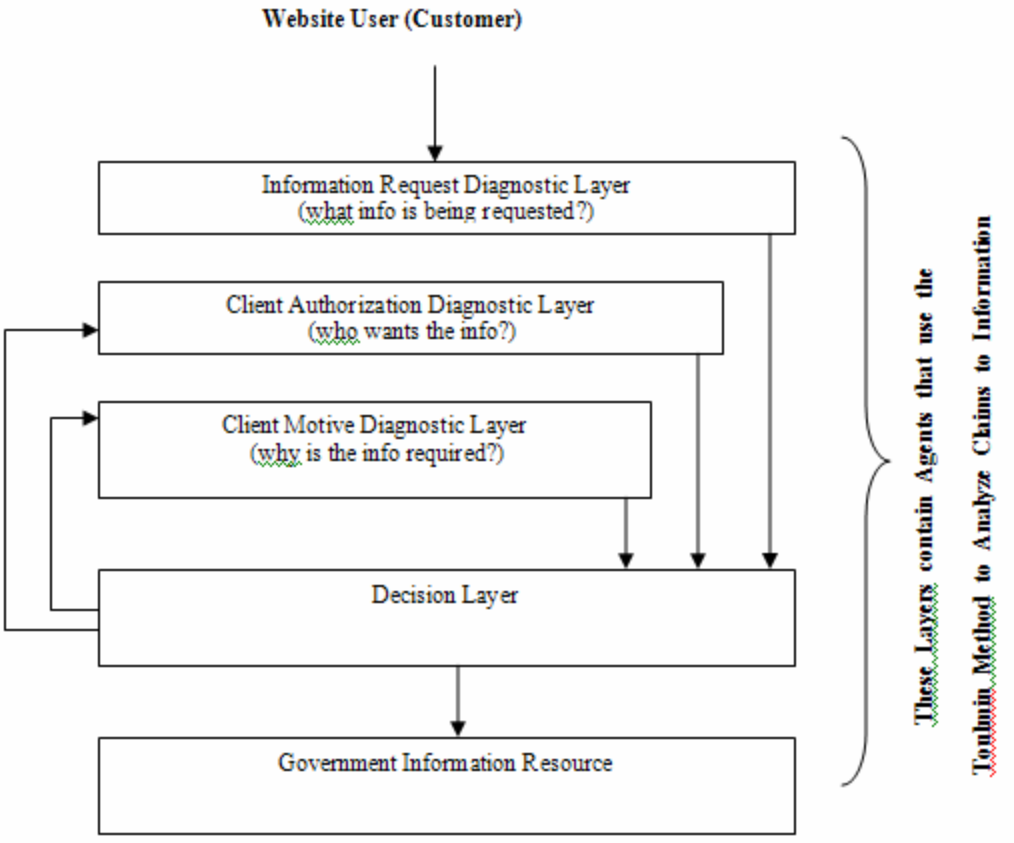

Fig. 2: The Proposed Framework

Structural parallels with the Toulmin method can now be seen to be properly emerging. The 'Data Agent' in the 'Client Authorization Diagnostic Layer' sends information about the requesting customer to the 'Decision Layer'.

In the 'Decision Layer', the 'Warrant Agent' then consults with the 'Backing Agent' to find out if this new 'data' (i.e. customer identification data – i.e. 'who' wants the information) can improve the validity of the claim to information. For the

sake of an example, let us say that the President of the USA is requesting the information. Such a scenario would in most cases improve the validity of the claim to information enough such that even if the request raised a red flag in the first round (because the information requested was sensitive), this new information, that the requester is the President, should make the claim valid, and the 'Decision Layer' should allow the request to pass through to the 'Government Information Resource'. Thus, in this second round of assessment, the Backing, Qualifier and Rebuttal Agents refer to client authorization databases and decision rules to assess how the new 'data', i.e. the identity of the client who is requesting the information, impacts the validity of the claim to information. The mechanism in this second round of assessment is similar to that described in detail earlier for the first round. Again, the 'Verdict Agent' judges the overall validity of the claim by weighing the assessments from the Data, Warrant, Backing, Qualifier and Rebuttal Agents. If the claim still raises a red flag (implying that the information on 'who' wanted the sensitive information was not enough to convince the 'Verdict Agent' that the request for online information should be honored) then the 'Verdict Agent' again requests the 'Warrant Agent' in the 'Decision Layer' to collect additional data on 'why' the claim is being made.

Thus the cycle described earlier repeats itself. This time the 'Warrant Agent' queries the 'Client Motive Diagnostic Layer' for information on the customer's motive for requesting the sensitive information. The 'Client Motive Diagnostic Layer' also contains a 'Data Agent' which finds out more information about why the customer is making the request for sensitive information. This is done by furnishing the customer with a form on which the customer indicates the reason for requesting the sensitive information. (the lines to depict this interaction have not been shown in figure 2 in order to reduce clutter).

Next, the 'Data Agent' in the 'Client Motive Diagnostic Layer' sends information about the motive for the request to the 'Decision Layer'.

In the 'Decision Layer', the 'Warrant Agent' then consults with the 'Backing Agent' to find out if this new 'data' (i.e. 'why' the client is requesting the sensitive information) can improve the validity of the claim to information. In this third round of assessment, the Backing, Qualifier and Rebuttal Agents refer to client motive databases and decision rules to assess how the new 'data', i.e. the client's motive for requesting the sensitive information, impacts the validity of the claim to information. The mechanism in this third round of assessment too is similar to that described in detail earlier for the first round. Again, the 'Verdict Agent' judges the overall validity of the claim by weighing the assessments from the Data, Warrant, Backing, Qualifier and Rebuttal Agents. If the claim is deemed valid, the customer is given access to the relevant 'Government Information Resource'. However, if the claim still raises a red flag (implying that the data on 'who' wanted the sensitive information and 'why' were not enough to convince the 'Verdict Agent' that the request for online information should be honored) then the 'Verdict Agent' refuses the customer online access to the relevant 'Government Information Resource'. However, this would not imply that the customer is being refused the information altogether. The customer may still be offered the opportunity to access the information offline via a visit to a physical archive. This option may be offered in those cases where the government is required to furnish the information under law (e.g. due to the Freedom of Information Act).

It should be noted that in addition to the layers and the agents, this framework also encompasses databases and decision rules that help the agents make assessments about 1) the sensitivity of information being sought, 2) the bonafides of the person making the request and 3) the motive for the request – i.e. whether the motive is legitimate or not.

CONCLUSIONS

This paper has sought to highlight the problem of vulnerability of information on U.S. government websites. It offers an agent-based framework that has the potential to allow the government to intelligently control the dissemination of information via government websites. The framework uses the Toulmin method to analyze the validity of claims to information. The advantage of the Toulmin method is that it is a widely established and accepted technique.

A key limitation of this paper is that it only presents a broad, skeletal framework and does not go into specifics of how the various components such as agents, etc., may be designed or put into practice. Nevertheless, by providing a descriptive framework, this paper provides a first step in the direction towards such future actualization.

Future research should attempt to determine how this framework can be made workable in practice; i.e. how the agents, databases and decision rules may be designed. Additionally, future research should also look at how to apply innovations to this framework. Two such innovations come to mind. Firstly, research should look at how to create self-destructing information (so that after a certain amount of time or due to some stimulus, sensitive information can self-destruct and vanish without a trace). Secondly, future research should look at how to educate customers about the sensitivity of the information that is provided to them so that they may also take precautions at their end to safeguard information.

REFERENCES

1. Aliev, Rafik A., Fazlollahi, B. and Vahidov, R. M. (2000) Soft computing based multi-agent marketing decision support system, *Journal of Intelligent & Fuzzy Systems*, 9, 1/2, 1-9.
2. Alison, L., Smith, M. D., Eastman, O. and Rainbow, L. (2003) Toulmin's Philosophy of Argument and its Relevance to Offender Profiling, *Psychology, Crime & Law*, 9, 2, 173-183.
3. Allegretti, C. L. and Frederick, J. N. (1995) A model for thinking critically about ethical issues, *Teaching of Psychology*, 22 1, 46-48.
4. Beck, R. J. and Wood, D. (1993) The Dialogic Socialization of Aggression in a Family's Court of Reason and Inquiry, *Discourse Processes*, 16, 3, 341-362.
5. Bivens, M. (2001) Nuclear Power and Terrorism, *The Nation*, October 25, 2000.
6. Boller, G.W., Sway, J.L. and Munch, J.M. (1990) Conceptualizing Argument Quality via Argument Structure, *Advances in Consumer Research*, 17, 1, 321-328.
7. Bonabeau, E. (2002) Predicting the Unpredictable, *Harvard Business Review*, 80, 3, 109-116.
8. Bozik, M. (1984) An Exercise in Inference Making, *Communication Education*, 33, 4, 401-403.
9. Braunack-Mayer, A. (2001) Casuistry as bioethical method: an empirical perspective, *Social Science & Medicine*, 53, 1, 71-81.
10. Chambers, T. (2000) Centering Bioethics, *Hastings Center Report*, 30, 1, 22-29.
11. Chambliss, M. J. (1995) Text cues and strategies successful readers use to construct the gist of lengthy written arguments, *Reading Research Quarterly*, 30, 4, 778-807.
12. Desharnais, P., Lu, J. and Radhakrishnan, T. (2002) Exploring agent support at the user interface in e-commerce applications, *International Journal on Digital Libraries*, 3, 4, 284-290.
13. Electronic Frontier Foundation, Chilling Effects of Anti-Terrorism (2003) http://www.eff.org/Privacy/Surveillance/Terrorism_militias/antiterrorism_chill.html.
14. Farmer, J. D. (1998) Scholarly communities and the discipline of the communication discipline, *Southern Communication Journal*, 63, 2, 169-172.
15. Fernandes, D., Gorr, W. and Krishnan, R. (2001) ServiceNet: An Agent Based Framework for One Stop E-Government Services, Proceedings of the Seventh Americas Conference on Information Systems, 1590-1594.
16. Freedom of Information Act (1966, with major amendments in 1974 and 1996) http://www.osc.gov/foia.htm.
17. Gasper, D.R. and George, R.V. (1998) Analyzing argumentation in planning and public policy: Assessing, improving, and transcending the Toulmin Model, *Environment & Planning B: Planning & Design*, 25, 3, 367-390.
18. Gold, J., Holman, D. and Thorpe, R. (2002) The Role of Argument Analysis and Story Telling in Facilitating Critical Thinking, *Management Learning*, 33, 3, 371-388.
19. Gregor, S. (1999) Explanations from Intelligent Systems: Theoretical Foundations and Implications for Practice, *MIS Quarterly*, 23, 4, 497-530.
20. Hicks, D. (1998) Narrative discourses as inner and outer word, *Language Arts*, 75, 1, 28-34.
21. Horton, R. (1998) The grammar of interpretive medicine, *Canadian Medical Association Journal*, 159, 3, 245-249.
22. Janssen, T. and Sage, A.P. (2000) A support system for multiple perspectives knowledge management and conflict resolution, *International Journal of Technology Management*, 19, 3-5, 472-490.
23. Jiménez-Aleixandre, M. (2002) Knowledge producers or knowledge consumers? Argumentation and decision making about environmental management, *International Journal of Science Education*, 24, 11, 1171-1190.
24. Jimez-Aleixandre, M. and Rodriguez, A.B. (2000) 'Doing the Lesson' or 'Doing Science': Argument in High School Genetics, *Science Education*, 84, 6, 757-792.
25. Johnson, D.E. (1995) Transactions in symbolic resources: A resource dependence model of congressional deliberation, *Sociological Perspectives*, 38, 2, 151-173.
26. Keenan, J.F. (1993) The function of the principle of double effect, *Theological Studies*, 54, 2, 294-315.

27. Kephart, J.O. and Greenwald, A.R. (2000) When Bots Collide, *Harvard Business Review*, 2000, 78, 4, 17-18.
28. Liu, S. (1998) Strategic scanning and interpretation revisiting: foundations for a software agent support system, *Industrial Management & Data Systems*, 98, 7/8, 362-372.
29. Locks, M.O. (1985) The Logic of Policy as Argument, *Management Science*, 1985, 31, 1, 109-109.
30. Lunsford, K.J. (2002) Contextualizing Toulmin's Model in the Writing Classroom: A Case Study, *Written Communication*, 19, 1, 109-175.
31. March, S., Hevner, A. and Ram, S. (2000) Research Commentary An Agenda for Information Technology Research in Heterogeneous and Distributed Environments, *Information Systems Research*, 11, 4, 327-341.
32. McBurney, P. and Parsons, S. (2001) Intelligent Systems to Support Deliberative Democracy in Environmental Regulation, *Information & Communications Technology Law*, 10, 1.
33. Moag, J.S. (1966) Field Logic and Communication, *Journal of Business Communication*, 3, 2, 11-13.
34. Novak, J.D. (1977) Theory of Education, Cornell University Press, Ithaca, New York.
35. Roberts, D.A. (1996) What counts as quality in qualitative research?, *Science Education*, 80, 3, 243-248.
36. Padovan, B., Sackmann, S., Eymann, T. and Pippow, I. (2002) A Prototype for an Agent-Based Secure Electronic Marketplace Including Reputation-Tracking Mechanisms, *International Journal of Electronic Commerce*, 6, 4, 93-113.
37. Paperwork Reduction Act (1995) http://www.cio.gov/Documents/paperwork_reduction_act_1995.html
38. Petta, P. and Müller, J. (2000) Guest Editorial, *Applied Artificial Intelligence*, 14, 7, 621-622.
39. Shultz, K. and Germeroth, D. (1998) Should We Laugh or Should We Cry? John Callahan's Humor as a Tool to Change Societal Attitudes Toward Disability, *Howard Journal of Communications*, 9, 3.
40. Stephan, M. and Rasmussen, C. (2002) Classroom mathematical practices in differential equations, *Journal of Mathematical Behavior*, 21, 4, 459-490.
41. Stranieri, A. and Zeleznikow, J. (2001) Copyright Regulation with Argumentation Agents, *Information & Communications Technology Law*, 10, 1.
42. Stranieri, A. (2002) An Argumentation Shell for Supporting the Development and Drafting of Legal Arguments, *Information & Communications Technology Law*, 11, 1, 75-86.
43. Stranieri, A., Yearwood, J. and Meikle, T. (2000) The Dependency of Discretion and Consistency on Knowledge Representation, *International Review of Law, Computers & Technology*, 14, 3, 325-340.
44. Teller, J. (2001) An on-line glossary as a way to foster the construction of a common culture among urban experts, stakeholders and decision-makers, *Construction Innovation*, 1, 4, 259-271.
45. Trent, J.D. (1968) Toulmin's Model of an Argument: An Examination and Extension, *Quarterly Journal of Speech*, 54, 3, 252-257.
46. Toulmin, S. (1958) The Uses of Argument, Cambridge University Press, Cambridge.
47. Watson, R. and Kay, K. (2002) Video Reveals Five more Bombers Ready to Strike, *The Times, London*, January 18, 2002.
48. Winters, Brian. (1998) Logic and Legitimacy: The Uses of Constitutional Argument, *Case Western Reserve Law Review*, 48, 2, 263-307.
49. Wenz, P. (1997) Philosophy class as commercial, *Environmental Ethics*, 19, 2, 205-216.
50. Whitenack, J.W. and Knipping, N. (2002) Argumentation, instructional design theory and students' mathematical learning: a case for coordinating interpretive lenses, *Journal of Mathematical Behavior*, 21, 4, 441-457.
51. Wooldridge, M. and Jennings, N.R. (1995) Intelligent Agents: Theory and Practice, *The Knowledge Engineering Review*, 10, 2, 115-152.
52. Wooldridge, M.J. and Jennings, N.R. (1999) Software engineering with agents: Pitfalls and pratfalls, *IEEE Internet Computing*, 3, 3, 20-27.
53. Young, M.F.D. (2000) Rescuing the Sociology of Educational Knowledge from the Extremes of Voice Discourse: towards a new theoretical basis for the sociology of the curriculum, *British Journal of Sociology of Education*, 21, 4, 523-536.