ABSTRACT
While millions of dollars have been invested in information technologies to improve intelligence information sharing among law enforcement agencies at the Federal, Tribal, State and Local levels, there remains a hesitation to share information between agencies. This lack of coordination hinders the ability to prevent and respond to crime and terrorism. Work to date has not produced solutions nor widely accepted paradigms for understanding the problem. Therefore, to enhance the current intelligence information sharing services between government entities, we have identified three major problem areas; Technical, Social, and Legal. Furthermore, we have developed a preliminary model and theory of intelligence information sharing through a literature review, experience and interviews with practitioners in the field. This model and theory should serve as a basic conceptual framework for further academic work and lead to further investigation and clarification of the identified factors and the degree of impact they exert on the system so that actionable solutions can be identified and implemented.

Categories and Subject Descriptors
K.4.3 Organizational Impacts - Computer-supported collaborative work.
K.6.4 System Management – Centralization/decentralization.

Keywords
Information sharing, collaboration, intelligence information, trust.

1. PROBLEMS AND MODEL
While millions of dollars have been invested in information technologies to improve information sharing capabilities among all law enforcement agencies, according to the National Security Agency there remains a hesitation to share intelligence information between agencies (Lieberman, 2007). This project aimed to identify barriers affecting effective information sharing between federal, tribal, state and local law enforcement agencies in the United States. Research in understanding these dynamics will lead to identification of actionable solutions to law enforcement intelligence information sharing across the federal, tribal, state and local levels.

To enhance the current intelligence information sharing services between government entities, we have identified three major problem areas; Technical, Social, and Legal. Furthermore, we have developed a preliminary model and theory of intelligence information sharing through a literature review, experience and interviews with practitioners in the field. Within each problem area we identified, individual factors were found that influence whether or not intelligence information is ultimately shared. Technical factors include interoperability, availability, and control issues. Social factors involve trust, shadow networks, and criticality issues. Finally, Legal factors are defined by considering local, state, and federal policies and their conflict.

Figure 1: Intelligence Information Sharing Factors

2. FRAMEWORK AND THEORY
Within this framework we describe two types of influences affecting whether or not sharing occurs; facilitators and detractors. This model is an offspring of Lewin’s force field analysis which is used here as a framework for looking at factors or forces influencing the decision of an individual or organization to share intelligence information (Thomas, 1985).
Technical issues such as having compatible operating systems, software, hardware, data definitions, secure access, control, high usability, system availability all can work towards improving the potential for information sharing but do not cause information to be shared (Lee & Rao, 2007; Scott, 2006). Regarding technology we may picture two young friends who tie two tin cans together on a string to communicate; it is not the technology of the cans that cause the two to talk across the string but their desire to share with each other that controls use of technology. It is therefore the social and cultural aspects of the relationship that matter more than the technology in the equation for information sharing. Today, the two kids from our example are texting.

Socially, greater trust and knowledge of the other parties involved lead to greater tendency towards intelligence information sharing. This involves agency culture and personal ties or connections with other involved agencies; which include shadow networking ties outside the workplace to include family and friend or other associations that involve one member having some other contact or relationship with someone associated with another agency (Drake, Steckler, & Koch, 2004b; “Information Sharing in and Across Government Agencies: The Role and Influence of Scientist, Politician, and Bureaucrat Subcultures -- Drake et al. 22 (1): 67 -- Social Science Computer Review,” n.d.; Marks & Sun, 2007). A ready example is family, friends or participation in clubs or activities which involve others apart from the work environment. These external contacts can have a positive influence on the likelihood of intelligence information sharing. Shared training and joint operations such as the U.S. Marshals joint fugitive round up effort with state and local agencies in Florida can have a positive effect on information sharing (Clark, 2008). Importance, as described previously, can be a very critical factor influencing the sharing of intelligence information as well. Information that is credible and which may result in some specific harm or loss is more readily shared and the pressure to share this information increased where there may be an approaching deadline (Lee & Rao, 2007).

In the area of legal influence, having a clear and enforced agency policy regarding intelligence information sharing will lead to the greater likelihood that information will be shared as will increased knowledge of laws and regulations which allow for intelligence information sharing. System governance and participation by others is also expected to be facilitator of intelligence information sharing where members and organizations have positive regard for and accept each other’s roles (Cresswell, Pardo, & Hassan, 2007). People within agencies are more likely to participate in systems that they have choice, investment and control over.

Facilitators include the positive influences that result from technical, social and legal rules, regulations, actions or perceptions.

Technical factors act as facilitators, driving movement toward information sharing, or detractors drawing momentum away from a choice to share intelligence information. Each of the factors under the headings given has a potential for facilitating or detracting from a choice to share intelligence information in a given context.

Technical issues such as having compatible operating systems, software, hardware, data definitions, secure access, control, high usability, system availability all can work towards improving the potential for information sharing but do not cause information to be shared (Lee & Rao, 2007; Scott, 2006). Regarding technology we may picture two young friends who tie two tin cans together on a string to communicate; it is not the technology of the cans that cause the two to talk across the string but their desire to share with each other that controls use of technology. It is therefore the social and cultural aspects of the relationship that matter more than the technology in the equation for information sharing. Today, the two kids from our example are texting.

Socially, greater trust and knowledge of the other parties involved lead to greater tendency towards intelligence information sharing. This involves agency culture and personal ties or connections with other involved agencies; which include shadow networking ties outside the workplace to include family and friend or other associations that involve one member having some other contact or relationship with someone associated with another agency (Drake, Steckler, & Koch, 2004b; “Information Sharing in and Across Government Agencies: The Role and Influence of Scientist, Politician, and Bureaucrat Subcultures -- Drake et al. 22 (1): 67 -- Social Science Computer Review,” n.d.; Marks & Sun, 2007). A ready example is family, friends or participation in clubs or activities which involve others apart from the work environment. These external contacts can have a positive influence on the likelihood of intelligence information sharing. Shared training and joint operations such as the U.S. Marshals joint fugitive round up effort with state and local agencies in Florida can have a positive effect on information sharing (Clark, 2008). Importance, as described previously, can be a very critical factor influencing the sharing of intelligence information as well. Information that is credible and which may result in some specific harm or loss is more readily shared and the pressure to share this information increased where there may be an approaching deadline (Lee & Rao, 2007).

In the area of legal influence, having a clear and enforced agency policy regarding intelligence information sharing will lead to the greater likelihood that information will be shared as will increased knowledge of laws and regulations which allow for intelligence information sharing. System governance and participation by others is also expected to be facilitator of intelligence information sharing where members and organizations have positive regard for and accept each other’s roles (Cresswell, Pardo, & Hassan, 2007). People within agencies are more likely to participate in systems that they have choice, investment and control over.

Detractors include negative influences resulting from technical, social and legal rules, regulations, actions or perceptions.

Detractors include negative influences resulting from technical, social and legal rules, regulations, actions or perceptions.

In the area of legal influence, having a clear and enforced agency policy regarding intelligence information sharing will lead to the greater likelihood that information will be shared as will increased knowledge of laws and regulations which allow for intelligence information sharing. System governance and participation by others is also expected to be facilitator of intelligence information sharing where members and organizations have positive regard for and accept each other’s roles (Cresswell, Pardo, & Hassan, 2007). People within agencies are more likely to participate in systems that they have choice, investment and control over.

Legal factors with a negative influence include security clearances which are not uniform or recognized across agencies, laws regarding privacy, secrecy or sharing of information that are conflicting or not well understood by participants. Social issues here involve issues of lack of trust, integrity, assurance or an agency culture which is geared towards not sharing (Lee & Rao, 2007). Trust is reduced where agencies compete for statistics, media attention and funding. Informal or outside contacts which are described as part of the shadow network have great potential to provide a negative influence if the information may be potentially damaging to an entity or person. Criticality includes timing of information and its potential impact so where there is little urgency the pressure to share this intelligence is reduced. Where there is no identified time frame or deadline the information may not be reacted to in a timely manner thus reducing the pressure to share this information. Lack of knowledge or inaccurate knowledge about what actions can be taken regarding sharing of information can hinder information sharing. Matters of jurisdiction, authority, and governance or control over the power or influence work against sharing (Drake, Steckler, & Koch, 2004a).

Technical factors act as detractors as well. Many agencies use different hardware and software programs for communication and information management and these may not interact together. Systems which are not responsive or show poor performance may not be adopted. Agencies with existing systems may not be financially able to change to more compatible or standardized systems. The costs for retraining onto new services can be high as well. Costs for maintenance of the systems must be considered.

These factors serve as the basis and framework for investigation. Inter-relationships of the identified factors influence the degree to which information sharing is more or less likely to occur and can be viewed as the balance of the result (see Figure 2 below).

Figure 2: Factors influencing the sharing of intelligence information

We are developing a formula and model based on this framework to describe and to predict resulting conditions regarding information sharing behaviors based on knowledge of the influencing factors. Probable effects from modifying the influencing factors are more readily apparent and easier to identify using such a model. The further investigation of these influences will inform the model as to the degree of influence each may have relative to the other so that decision makers can pattern solutions towards desired ends.
3. RESEARCH CONTRIBUTIONS

By using the model developed we can visualize the effects of making changes in different areas and observe the outcomes. We can see how adjustments in degree of influence for the influencing factors identified determine whether or not intelligence information is shared under the given circumstances. This leads to the theory that intelligence information sharing between law enforcement agencies is affected by technical, social and legal factors which are comprised of issues of interoperability, availability, control, trust, shadow networks, criticality, knowledge, and governance. We have identified the major problem areas and posit that these factors work to facilitate or detract from the sharing of intelligence information between agencies.

This model and theory should serve as a basic conceptual framework for further academic work and lead to further investigation and clarification of the identified factors and the degree of impact they exert on the system so that actionable solutions can be identified and implemented.

4. ACKNOWLEDGMENTS

Our thanks go out to the 2009 iConference reviewers for their constructive recommendations and comments on this work. The views and ideas expressed here are of the authors alone and do not reflect the views or policies of the iConference personnel.

5. REFERENCES


