Collaborative Cross-Border Security Infrastructure and Systems:
Identifying Policy, Managerial and Technological Challenges

Luis Felipe Luna-Reyes, Department of Business, Universidad de las Américas Puebla, San Andres Cholula, Puebla, Mexico

Douglas C. Derrick, School of Interdisciplinary Informatics, University of Nebraska at Omaha, Omaha, NE, USA

Brent Langhals, The Air Force Institute of Technology, United States Air Force, Wright-Patterson AFB, OH, USA

Jay F. Nunamaker Jr., Center for the Management of Information & National Center for Border Security and Immigration, The University of Arizona, Tucson, AZ

ABSTRACT

A long-standing problem in the US-Mexico bilateral agenda is migration. Although both countries have important agreements to promote economic exchange and trade, the events of 9/11 and other acts of terrorism have increased concerns about border security. Since the US-Mexico border is one of the most important borders in the world in terms of activity, securing it without interfering with the legitimate flow of people and goods, poses an important challenge. The purpose of this paper is to propose conceptual frameworks and models to facilitate collaboration across national borders, by discussing and considering key factors for collaborative US-Mexico Border Security Infrastructure and Systems. Border security technical solutions pose an interesting domain because there are a myriad of concerns (e.g., political, economic, social and cultural) outside the technical implementation that must be deliberated and examined. In this conceptual study, unique aspects of trust, governance, information sharing, culture, and technical infrastructure are identified as the key ingredients in a cross-border collaboration effort. A bi-national organizational network appears to be an effective institutional design to develop a better understanding of the problem, as well as required policies and technologies. This approach is consistent with experiments, research, and conclusions found in the European Union.

Keywords: *Cross-Border Information Technology, Information Systems, Interorganizational Collaboration, Policy-Technology Integration, US-Mexico Border*

DOI: 10.4018/jep.2013040102

INTRODUCTION

Cross border collaboration is required in order to solve the common complex problems of the modern world. The globalization process and the establishment of international free trade agreements are increasing the need for new ways to collaborate across national boundaries around the world. In fact, this trend has been transforming the mission and main objectives of customs administration, which now include promoting global competitiveness (Maldonado Carrasco, 2009; Vogel, Schmidt, Lemm, & Österle, 2008). Studying borders has a long tradition, and these recent phenomena, plus the rise of international terrorism, have renewed interest in border studies. For example, the North American Free Trade Agreement (NAFTA) was signed to promote commercial interchange between Mexico, Canada and the United States. Although NAFTA emphasizes free trade, the 9/11 terrorist attacks on the US have increased concerns about border security and the ability to screen large volumes of trucks at commercial ports of entry. Moreover, immigration has been a longstanding concern for both Mexico and the United States. The convergence of border security, immigration and trade represents a dynamic and complex issue. Moreover, the political clout of local border communities, together with the interplay of these local interests with state and federal interests has an impact on both the debate and implementation of policies related to this complex issue. The border environment has unique political, social and economic challenges for effective transnational collaboration. Thus, the value of investing in information systems and information technology in the border environment lies in the ability to facilitate trade and maintain security in a politically acceptable way. In this sense, although introducing technologies at the border has the potential of transforming current activities (e.g., increasing competitiveness), the selection and implementation of information technologies at the border is not only a technical-economic process, but also a social and political one (Dawes, Cresswell, & Pardo, 2009; Livermore & Rippa, 2011).

In order to meet the daunting challenge of facilitating trade and securing borders, it is becoming apparent that effective border security can only result from effective cross-national collaboration (Henningsson, Gal, Bjørn-Andersen, & Yao-Hua, 2011). Accordingly, trust, information sharing, technical infrastructure and cultural understanding become the cornerstones of successful cross-border collaborative efforts. On the basis of a literature review on border theory and interorganizational collaboration and governance, as well as fieldwork at the US-Mexican border, the purpose of this paper is to propose a process model that integrates technical development and policy development process in order to facilitate collaboration across national borders. Our model is a feasible way of developing technologies that respond to the social, economic and political issues associated with cross-border collaboration. We highlight key challenges and factors that must be considered for collaborative US-Mexico Border Security Infrastructure and Systems, and we also discuss societal and political issues involved in cross-border collaboration. Our guiding questions for the study are what is the current status of technology and systems infrastructure at the US-Mexico border? And which processes and frameworks may help build effective cross-national systems? Collaborative cross-border security infrastructure and systems is one aspect of Government to Business (G2B) interorganizational systems that is under-reported in the academic literature (Rukanova, van Stijn, Henriksen, Baida, & Yao-Hua, 2009). This paper attempts to fill this gap by exploring policy, managerial and technical challenges associated with developing such systems.

The paper is organized in five interrelated sections. First, we present some particularities of the US Mexico border and two frameworks to understand information sharing and collabo-

ration at national borders. After introducing these frameworks, we present fieldwork and data to contribute to the understanding of the current status of border systems. As a result of this work, we present five key challenges for border security. Finally, the paper finishes with a proposed model to integrate policy and technology development and concludes with some policy recommendations and considerations for future research.

UNDERSTANDING INTERNATIONAL CROSS-BORDER COLLABORATION

As mentioned in the introduction, border studies have a long tradition. Moreover, research to understand cross-boundary, inter-organizational collaboration has also developed a core literature. In this section of the paper, we introduce some context for the US-Mexico border, and then discuss relevant concepts and frameworks from border studies and cross-boundary collaboration literature.

The Unites States - Mexico Border

The Mexico-US border constitutes one of the most important borders around the world in terms of activity. It extends for 3,200 Km, involving 39 Mexican Municipalities, 25 US Counties and 14 twin cities, with a total population of 10.5 million people. The border between the two Countries is the world's most frequently crossed border with 250 million legal crossings and an estimated 50 million illegal crossings yearly. It contains 25 Ports of Entry and in 2008, almost 4.9 million trucks from Mexico crossed into the US (US Department of Transportation, 2008). From an economic perspective, Mexico is the second only to Canada as the largest trading partner of the United States accounting for $584 billion worth of trade annually (Kingsbury et al., 2002). Added to this huge volume of legal commerce, there is the persistent problem of illegal border crossings. In the first six months of fiscal year 2009, the Tucson sector of the Customs and Border Protection (CBP) detained over 98,000 illegal immigrants attempting to enter the US, which accounted for 34% of all illegal immigrants caught in the southwestern US during this time period (CBP, 2009). Additionally, another important security-related border problem is related to the traffic of drug and guns in the border. It is estimated that every year approximately 18-39 billion dollars are moved from the interior of the United States to drug trafficking organizations from Colombia and Mexico through the US Southwest border (Perkins & Placido, 2010). In recent years, efforts from the Mexican government have led to an increase in drug-related violence, particularly close to the US-Mexico border (Perkins & Placido, 2010). Consequently, one of the most challenging and important aspects of border security is distinguishing "criminals" from non-threatening economic refugees, while at the same time limiting interference with legal and vital commerce. These statistics clearly demonstrate the competing interests between allowing access for lawful economic and immigration purposes and securing the border against illegal activity.

Border Theory

According to a recent study, border related research and discussion may benefit from a guiding framework (Brunet-Jailly, 2005). The Border Theory proposed by Brunet-Jailly (2005) suggests that there are at least four predominant lenses to understand national borders.

First, the theoretical framework suggests that there is a set of common cultural values related to border communities that define them as a localized society such as religion, a sense of community, or similar socio-economic background. For example, although it is common to stress cultural differences between Mexican and US counterparts across the borders, many of these analyses fail to recognize an important set of common cultural characteristics in border states (Velázquez García, 2008). Border States shared a common history until the first half of the 19th Century, when for different reasons, portions of the Mexican territory became US

territories and later US states. Although social and cultural dynamics have contributed to build a perception of risk associated with differences among border inhabitants, people from Ciudad Juarez, Mexico are more similar to people from El Paso, US (i.e., twin cities at the US-Mexico border) than they are to those from Mexico City.

The second component of Brunet-Jailly theory consists of the Political Clout of Cross-Border Communities, composed by local civic and political organizations. These organizations and their objectives represent the main concerns of local communities at the border (e.g. environmental, economic development, violence, drug trafficking, health or migration). The third component of the theory employs an Economic Lens, and it involves the cross-border flow of goods, people and investment. As mentioned in the introduction, the US-Mexico border has very intense activity in terms of the flow of people and goods. Moreover, because of the differences in labor costs and regulations between the two countries, an important flow of investment moves from the US to Mexico. Investment in the manufacturing industry, the IT services industry and the energy sector have contributed to increased regional economic integration at the border, creating what some authors have called a "shared space" (Washburn, 2004). Finally, the last component of the proposed border theory considers the relationships among private and public organizations at the local, state and federal level. These relationships constitute networks of organizations that work for the accomplishment of shared goals (e.g., monitoring environmental issues) or specific tasks (e.g., controlling the transit of goods or people).

The four lenses involved in the Theory of Borders proposed by Brunet-Jailly imply complex relationships and interactions among individual actors, public and private organizations as well as non-profit groups. For instance, the analysis of market forces and trade flows implies communication among immigration and customs authorities in both countries, private companies involved in economic transactions such as suppliers and transportation companies, as well as non-profit groups with concerns associated with human rights, labor rights, or the environment. Similarly, local, state and federal agencies need to coordinate with the private sector to find solutions to drug and guns trafficking, as well as to problems of violence related to these activities. Problems related to such complex systems require innovative and flexible solutions, which no longer can be managed by the classic bureaucratic structure in government, but through the collaboration of organizational networks (Gascó, 2004; Goldsmith & Eggers, 2004). Given the importance of information technologies to facilitate collaboration inside networks, Navarrete and her colleagues (2009) propose an extension of the Theory of Borders that includes an Information Sharing component, which encompasses trusted social networks, shared tacit and explicit knowledge, and an integrated data infrastructure (Dawes, Cresswell, & Pardo, 2009; Pardo, Gil-Garcia, & Luna-Reyes, 2008).

Although research on transnational organizational networks is scarce, it may be similar to organizational networks in cross-organizational relationships in other policy contexts (Cresswell, Burke, & Navarrete, 2009). Usually, these relationships constitute social networks in which individuals rely on each other to accomplish their goals. Trust, which comes from different sources and takes different forms during the relationship, plays an important role in these networks (Dawes et al., 2009; Luna-Reyes, Cresswell, & Richardson, 2004; Rousseau, Sitkin, Burt, & Camerer, 1998). Early in a relationship, trust is frequently built on the perception of risks and benefits associated with the interaction (i.e., calculative trust). As the relationship evolves, the calculative component is gradually substituted by a knowledge-based component, which involves positive and negative experiences in the interaction. Moreover,

at any time in the relationship, trust can be based on an institutional component, which is usually materialized in the form of contracts, formal agreements or legal frameworks. This institutional component may play an important role in the early stages of a relationship because it reduces the perception of risk or improves the legitimacy of the network.

Social networks also need to share knowledge about problems and their potential solutions. Knowledge has two dimensions, an explicit dimension, which is written in documents databases and other objects, and a tacit dimension, which is embedded in practice. This tacit dimension of knowledge is hard to be shared and it has the potential to be a barrier to knowledge sharing about a particular problem situation (Carlile, 2002; Luna-Reyes, Black, Cresswell, & Pardo, 2008). Research in the area suggests that effective knowledge sharing across cultural and organizational boundaries can be facilitated by Boundary Objects, which are "objects that are shared and shareable across different problem solving contexts" (Carlile, 2002). Examples of boundary objects are repositories, forms and methods, models or maps of boundaries.

A last component included in the framework is an Integrated Data Infrastructure, which is frequently associated with the concept of interoperability. Interoperability can be defined as "the mix of policy, management, and technology capabilities (e.g., governance, decision making, resource management, standards setting, and Information Technologies) needed in order for a network of organizations to operate effectively" (Pardo et al., 2008). Interoperability delivers value through the potential creation of new knowledge on the basis of the integration of information from multiple sources across organizational boundaries. In order to build interoperable systems, many different "borders" must be crossed (e.g. data or process integration).

Interorganizational Collaboration and Governance

As highlighted in the previous section, better cross-border coordination and information sharing constitute some of the key challenges for effective collaboration. In this section, we will introduce previous research in similar contexts and a model to address coordination and governance problems across the border.

In an attempt to respond to the challenges of global trade and security, the European Union (EU) has funded and developed the Information Technology for Adoption and Intelligent Design for eGovernment project (ITAIDE). The main objective of the project was to develop innovative eCustoms solutions (Henningsson et al., 2011; Henningsson, Rukanova, & Hrastinski, 2010; Vogel et al., 2008). The project was developed under the design science research approach, in which the research team has the objective of "producing theory for guided action to achieve some expected outcome" (Tan, Bjorn-Andersen, & Henningsson, 2010, p. 2). The project involved the creation of four "*Living Labs*" in four countries in the European Union. Each Lab involved the collaboration of tax and customs administrations, IT providers, private companies and universities, working together to define problems and to develop and test feasible solutions. The effort has yielded insights about the design of organizational, human and technological components of an eCustoms solution, including interesting concepts such as a "trusted trader" (Henningsson et al., 2011), resource dependencies inside the organizational network (Henningsson et al., 2010), interdependencies and activities among different levels of government and interorganizational systems (Rukanova et al., 2009), adoption and acceptance of the technology (Raus et al., 2010), and the need of standards for interoperability (Vogel et al., 2008). Although the context of the EU is different from the US-Mexican context,

it is especially interesting the collaborative approach illustrated by the ITAIDE project as an alternative way to find solutions for cross-border security.

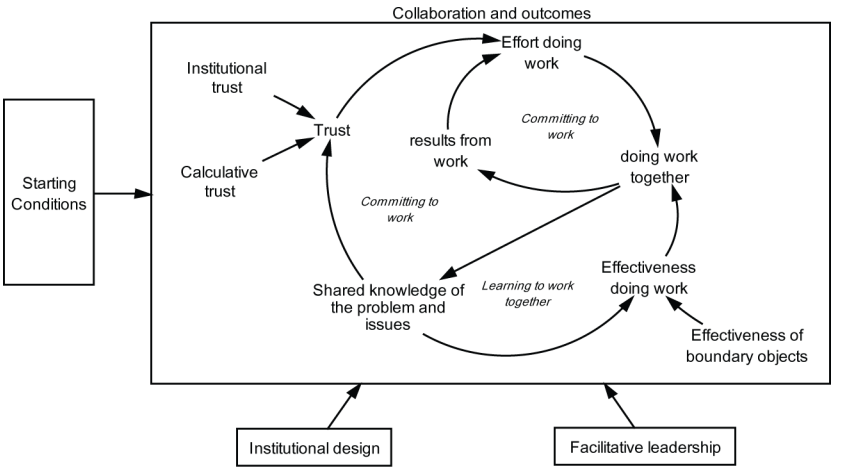
As a result of their work in governance and collaboration, Ansell and Gash (2007) developed a model to guide the collaboration processes across organizational boundaries (see Figure 1). The model comprises five main components: starting conditions, institutional design, facilitative leadership, collaborative processes and outcomes.

The starting conditions refer to the main incentives and constraints on participating in a collaborative effort. These incentives are formed by a series of asymmetries in terms of power, resources and knowledge as well as previous history of collaboration among partners. There are many asymmetries in the US-Mexico border in terms of technology and power (Olson, 2010). Understanding the differences between the two sides of the border plays an important role in developing a technical infrastructure to support effective collaboration. It is likely that the perception of the usefulness of technology to solve the problem will vary from one side of the border to the other, and also when considering different levels of government (i.e., local, state, federal). The history of collaboration between the two countries has varied over time from armed conflicts to close relationship of regular interchange. Recent bilateral agreements between the two countries, as well as some successes in in sharing information to facilitate the free transit of goods and people are important signs of the intent and need to collaborate (Benítez Manaut & Rodríguez Ulloa, 2006). These international agreements constitute important sources of institutional trust, are a needed to start effective collaboration.

A second important element in the model considers institutional design. Such institutional design involves the main rules to make decisions, design policies, network structure, and assessment mechanisms (Goldsmith & Eggers, 2004). This element suggests that collaboration inside the networks needs to be managed in a participatory and transparent way. For example, US authorities may desire for Mexican authorities to pre-screen people or goods attempting to cross the border, but the Mexican constitution considers free transit as a basic citizen right.[1] Solving this difference presents a clear dilemma.

A third important component of the model involves facilitative leadership. The role of the leader is important in public administration, particularly in contexts like the borders (Crosby & Bryson, 2005; Frederickson, 2005). A leader

Figure 1. A model for Collaborative Governance. Adapted from Ansell and Gash (2007).



in this environment has new roles to play, such as designing a vision, policies and learning processes that enable knowledge utilization and promotes more insightful views of a current problem. Finally, the leader is a steward of the people's needs and the broader mission (Bertucci, 2006).

The fourth component involves the collaboration process itself. The collaboration process depicted in Figure 1 is similar to other representations existing in the literature, and constitutes a set of virtuous cycles where collaboration brings trust and commitment among participants, and also shared understanding about the problem area. However, most virtuous cycles are also potential traps. In other words, when there is no trust, people will not develop commitment or shared understanding, and it is not likely to get an outcome. Current research shows that the institutional component of trust (like the agreements between countries) constitutes a necessary condition, which unfortunately is not always sufficient. In many cases, trust starts building when participants understand the benefits of the collaboration and experience early positive results. In this way, the results from work included in Figure 1 have proven to effectively start or accelerate the process of collaboration. Results from work not only include objects, but also the development of capabilities to collaborate (Dawes et al., 2009). As we suggested in previous paragraphs, building necessary understanding and trust is particularly difficult to accomplish when institutional designs are incompatible or even contradictory. Moreover, social, economic and political factors are all potential sources of these contradictions that may difficult collaboration.

The frameworks provided in this section provide a set of ideas to organize conversations and research related to collaboration at the border. Problems related to border security infrastructure and systems are varied and include water management, air pollution, trade or migration, amongst others. In this paper we will focus on only one of these difficult policy areas: migration. However, we believe that the general recommendations emerging from this analysis may apply to other problems at the border.

METHODS AND DATA

Migration policy and technology consists of both facilitating the legitimate flow of people and restricting the unlawful flow of individuals. To this end, numerous studies have proposed a wide range of new technologies that may improve border agent's ability to detect and apprehend illegal immigrants, particularly the criminal elements (Ackleson, 2005; Bracchi, Cukic, & Cortellessa, 2006; Burgoon et al., 2009). In order to better understand these technologies and their applications and as part of ongoing border security research, from February to November of 2009, we conducted an extensive field study with agents from Customs and Border Protection, Border Patrol, Immigrations and Customs Enforcement, and the Federal Bureau of Investigation. The study began with a series of meetings hosted at the University of Arizona where representatives from the various agencies discussed issues they face in their daily work. Using the results from these initial meetings, we followed up with visits to Border Patrol's Tucson Sector Headquarters, the Nogales port-of-entry, and field agent stations throughout the Tucson sector to conduct interviews. Interviews contained a series of predetermined questions as well as questions that were developed based upon information obtained during the visits.

Over the duration of the field study, we were granted access to 57 individuals ranging from high-level sector chiefs to agents working daily operations in the field. In order to ensure each agent candidly responded to our questions, agents were promised anonymity that was enforced by replacing agent names and specific organizations with randomly assigned interview numbers within the database holding interview

answers. The goal of each visit was to gain a better understanding of the conditions under which the US Border Patrol works as well as the technologies they commonly use in the field.

Finally, to wrap up the field study, we received several briefings from Customs and Border Protection agents. These briefings highlighted the issues customs personnel face as well as their many areas of responsibility. Again, the goal was to better understand the kinds of technology customs agents routinely use and what future technologies they would like to have. The following section highlights key technologies and challenges identified by border security agents who participated in the field study, but should not be construed as a comprehensive list of the technologies used by border security agents or as a complete list of the challenges they face. Instead they represent potential themes that are likely to come up in any US-Mexico collaboration efforts. We also include the Mexican perspective based mainly on current plans of the Customs Administration. However, the information is very limited, and it constitutes a current weakness of our work.

KEY TECHNOLOGIES AND CHALLENGES AT THE BORDER

To execute its various missions, US Customs and Border Protection (CBP) maintain and utilize several databases. The US administers the US Visitor and Immigrant Status Indicator Technology (US-VISIT) program, which requires all incoming non-immigrant aliens to submit to a biometric scan. The multibillion dollar US-VISIT program takes two index fingerprint images from each visa applicant and matches these prints against those of several hundred million visa holders to detect whether the new applicant already has a visa under a different identity (Wein & Baveja, 2005). Additionally, CBP administers the Container Security Initiative, a program in which CBP inspectors screen US-bound marine containers at foreign ports of loading around the world. The Secure Electronic Network for Travelers Rapid Inspection (SENTRI) system allows users to generally bypass the inspection process. Participants must pass criminal background checks and pay a fee to enroll. Currently, over 42,000 travelers participate in the SENTRI program along the US–Mexico border, a number that has increased following 9/11 (Ackleson, 2005).

Finally, CBP manages an interagency database called E3. This database is a comprehensive system linking all CBP stations that tracks photos, fingerprints, and biographical information for every illegal immigrant apprehended in the US. CBP uses this database to identify repeat offenders as well as to help identify criminals when they are recaptured. Unfortunately, additional homemade database systems are pervasive throughout the Border Security environment. Agents have developed limited use (primarily Microsoft Access based) databases to track everything from prosecution documents to forfeiture/vehicle seizure assets. Unfortunately, these databases are not linked or distributed and may or may not contain updated information. These databases often serve limited purposes, but may contain vital information that would be useful if they could be shared across all agencies. One of the primary goals mentioned by the agents interviewed was to consolidate databases.

The Border Patrol also operates an extensive network of sensor devices comprised of motion, thermal, video and seismic equipment. Information from these devices is fed back to station command centers where agents monitor the systems 24 hours a day, 7 days a week. When a sensor is "*tripped"* the agents focus resources on the area to determine the cause. In the border environment it is not uncommon for animals, including cattle, to cause the alarms to go off. If the agent in the command center is unable to determine the cause, he or she will direct agents to the location. Throughout the interviews, agents emphasized a need for better surveillance equipment or "smart" technology that will help them remotely assess causes of

sensor alarms. Such a system would allow improved utilization of human resources as it often takes Border Agents hours to reach the sensor sites.

The Border Patrol recently began employing Mobile Surveillance Systems (MSS). The MSS is a truck-based platform armed with thermal imaging, ground radar, laser range finder, and high-resolution video cameras. Unfortunately, data from the MSS is not easily transmitted to the nearest stations. As a result, these systems must be manned full time and nearby Border Agent activities directed by the MSS crew. Additionally, data from the MSS is not stored for future analysis. Border Agents would like to have the ability to forward the data to the Tucson Sector HQ for pattern analysis. Despite these shortcomings, the MSS is a valuable tool and accounts for a significant portion of all illegal crossers apprehended miles away from the border.

Customs also operates a variety of technologies that help them identify vehicles, people, or smuggled items attempting to cross the border. One such technology is the Automated Targeting System (ATS). As the cornerstone for all CBP targeting efforts, ATS assigns a "risk assessment" to every person and container seeking to enter or exit the US Originally established to assess cargo that may pose a threat to the US, the Department of Homeland Security (DHS) has expanded its use to establish risk profiles for passengers and private vehicles. CBP uses ATS to improve the collection, use, analysis, and dissemination of information that is gathered for the primary purpose of targeting, identifying, and preventing potential terrorists and terrorist weapons from entering the US. It is a weighted system that searches an extensive database and presents the probability that a vehicle or passenger presents a risk. Every traveler and all shipments are processed through ATS, and are subject to a real-time rule based evaluation. ATS receives various data in real time from the following different CBP mainframe systems, such as the Automated Commercial System (ACS) or the Automated Export System (AES). Lastly, ATS collects data from foreign governments and certain express consignment services in conjunction with specific cooperative programs.

In addition to its risk-based assessment system, ATS provide a graphical user interface (GUI) for many of the underlying legacy systems from which ATS pulls information. This interface improves the user experience by providing the same functionality in a more rigidly controlled access environment than the underlying system. This system has proven effective to help identify individuals smuggling drugs and humans into the United States. For large vehicles such as semis and trucks, customs also operate a Vehicle Inspection X-Ray System. This system can be fixed at the border crossing or mobile (truck based). The X-rays taken by this system are capable of detecting drugs, smuggling, or other illicit material (such as banned agriculture items) that have been hidden in a vehicle. When a suspicious X-ray is viewed, agents conduct further hands-on searches, often with aid from drug/bomb sniffing dogs.

On the Mexican side of the border, two are the main systems in use. The Customs Automated System (SAAI), which keeps track of imports and exports, and the Vehicular Control System (SIAVE), which was recently implemented to identify vehicles carrying guns or other illegal products into the Country (Secretaría de Hacienda y Crédito Público, 2007). During the last years, new screening technologies have been installed in four pilot sites in the country, but there is still an important need to invest in infrastructure to improve customs administration activities. There is currently an ambitious plan to invest in the necessary infrastructure, which has started with investments in buildings and other facilities (Secretaría de Hacienda y Crédito Público, 2007).

KEY CHALLENGES AT THE BORDER

In addition to identifying the key border security technologies listed above, the field study also sought to determine specific issues currently impacting security operations at the border. As part of the initial meetings at the University of Arizona, agents from each organization collaborated to identify the top ten challenges facing border security personnel in the field. Subsequently, individual agents were asked to rank each challenge based upon personal experiences and provide specific examples to support their ranking. From their responses, we identified common areas of concern that could potentially impact US-Mexico collaboration efforts. Table 1 summarizes the top ten issues with the hopes that it will spur discussion on how these issues can be addressed from a multinational viewpoint as well as illuminate potential problems in US-Mexico collaboration. Subsequent sections provide additional detail for the top five.

First of all, without exception, all agents we interviewed called for better inter-agency coordination, especially when it comes to information sharing. Roles and responsibilities in the field are fairly well defined. However the agents believe that better coordination at political and other high levels of leadership would improve information sharing, resource allocation and planning. The agents' concerns were specifically addressed toward internal US agency coordination, but this issue is likely to be a thorny one for cross-national organizations as well. While several agents admitted that limited information sharing with Mexican authorities exists, most interviewed expressed reservations about the amount and type of information being shared.

The second most prominent issue identified by border security agents is IT system integration, especially when it involved managing disparate databases. Every organization within Homeland Security develops and maintains their own set of databases for tracking information relevant to their organization. Each organization is also very protective of who can access their information. Worse still, when one database is updated, related information in another database is not automatically updated. Also, when a database is shared, it is not integrated, thus forcing agents to use multiple login/password combinations and hindering efficient information sharing. Agents reported that due to lack of access to all databases they occasionally were unable to ascertain the legal status of migrants entering the country, particularly if the migrant has a criminal record. Unfortunately, sharing this data and databases across borders and governments is even more problematic.

Table 1. Top 10 agent concerns for border security operations

Rank	Category	Avg. Rank	STD
1	Inter-agency Collaboration	2.17	2.25
2	IT System Integration	3.67	1.72
3	Communication Technologies	4.67	2.87
4	Process Improvements (including SOP revisions)	5.25	2.77
5	Technological Tool Development (including detection tools)	5.39	2.67
6	Political Advising & Policy Revision	6.00	3.93
7	IT System Development	6.30	2.30
8	Managerial Realignment	6.58	3.20
9	Training Curriculum Improvements	6.67	2.10
10	Security and Systems Protection	7.75	2.05

The third biggest security concern is field communications. Current improvements in securing communications had the unfortunate byproduct of occasional communication outages. Further complicating the issue is that many border security agencies cannot talk directly to local law enforcement. As a result, many agents carry field radios, cell phones, and blackberries to enable mobile communication with everyone with whom they need to coordinate. All agents interviewed requested a single, reliable voice and data communications system for use in the field. In terms of data communications, numerous agents expressed the need to transmit and store large amounts of video, sensor, and biographical data (fingerprints/photos) for future analysis, which is not adequately supported by the current architecture, particularly between individual agents in mobile vehicles and station headquarters. Cross border communication poses an entirely different set of technical, policy and security concerns.

The fourth major issue agents stressed was the fact that Standard Operating Procedures need to be improved, particularly when multiple agencies are involved. This often is a highly political issue, especially when the coordination involves processing, detention, prosecution and/or deportation of illegal immigrants. Each agency theoretically obeys the same DHS directives and US laws, but interpretation of what is acceptable in the field can vary between organizations. The agents would like stronger leadership and inter-agency cohesion in this area.

Finally, for the fifth concern, agents indicated they would like to see technology fielded that will aid in the detection of hostile intent, criminal backgrounds, or even outright deception when interviewing apprehended illegal immigrants, especially in the field. The agents' concern was that whatever technology is developed must be practical, useful, and impose no additional burden on the already over-tasked agents.

In Mexico, the 2007-2012 Plan for Customs Modernization (Secretaría de Hacienda y Crédito Público, 2007), the Customs Mexican Administration recognized the following important challenges: the lack of a shared strategy among key agencies, problems related to process improvement and organizational redesign, and problems related with fragmented information and outdated information systems. In contrast to their American counterparts, Mexican authorities also stress the need of improving the regulatory and legal frameworks as a challenge. There was much less concern related to the screening of individuals because there is almost no screening for people who crosses the border from the US into Mexico (Olson, 2010).

A MODEL FOR INTEGRATING POLICY AND TECHNOLOGY DEVELOPMENT

As demonstrated in the previous section, there are a multitude of issues and challenges involved in improving border security. However, we believe that in order to develop appropriate solutions for the challenges, we need to develop more specific modes of collaboration to coordinate the implementation of policy and technology at the border. Obviously the development of the innovative technologies will not alone solve border security issues, especially in a multinational collaboration environment with frequently asynchronous technological capabilities. Likewise, no single policy decision will remedy all border security problems. However, it is possible that effective integration of technology with border-related policies may significantly improve the desired impact of both. Unfortunately in the past, policy decisions and technology development have taken divergent paths, with one ultimately undermining the other. Therefore, we propose a new model for US-Mexico collaboration that blends the policy making process with the process of developing emerging technologies to enhance effective decisions at the border. In order to be effective, the process presented in this framework needs to take place inside a network of organizations from both sides of the border, including representatives from the public and

private sectors, local, state and federal governments, universities, research centers, as well as the public (Ansell & Gash, 2007; Dawes et al., 2009). The process involves and is influenced by political and economical factors both inside the network of organizations and from the context where the network operates.

Policy Development Considerations

Border security policy development has proven to be a constant and continuous endeavor, undertaken with the presumed goal of benefiting all actors on both sides of the border. It involves considering social, economic, legal, and environmental issues and often requires delicately balancing competing interests in order to ensure the public good (Benítez Manaut & Rodríguez Ulloa, 2006). Looking at these issues through the theoretical lenses of the extension of the Brunet-Jailly theory and previous experiences on other border problems (Cresswell et al., 2009; Navarrete et al., 2009), indicates that some of the trust issues can be overcome by developing bi-national agreements that promote changes in the incentive structures of organizations working across borders. The purpose of these incentives is to facilitate collaboration. Moreover, by establishing and working in the legitimacy of transnational inter-organizational networks, these networks can work through the technical and social issues related to information sharing. Trust and knowledge develops inside the network thereby creating value to the communities involved in the problem. Policy decisions can have enormous impacts on the types of technology developed and how they are implemented.

For the purposes of this paper and development of our proposed model, policy development can be broken down into the following three steps. First, we clearly need to verify, define, and detail the problem. Many times the border security objectives are not clear or even contradictory. Moreover, stakeholders frequently have competing values related to the problem and feasible solutions. Clearly, identifying the problem to be resolved requires the identification of main stakeholders who need to build understanding about the problem and realistic evaluation criteria (such as cost, net benefit, effectiveness, efficiency, equity, administrative ease, legality, and political acceptability). Finally, we must adequately identify alternative policies.

The second step consists of policy implementation. Implementation is a deliberate and sequential set of activities directed toward putting a policy into effect. It consists of organized activities by the core network of key stakeholders toward the achievement of goals and objectives articulated in authorized policy statements. Finally, policies need to be evaluated. Although policy evaluation is quite rare because of political reasons, an important component of the policy process involves assessing the effectiveness of both the policy itself and the associated technologies created to support its implementation. Policy evaluation may ask deep and wide-ranging questions, such as: Was the problem correctly identified? Were any important aspects overlooked? Were any important data left out of the analysis? If so, did this influence the analysis? Were recommendations properly implemented? Is the policy having the desired effect? Are there any needs for modification, change, or re-design? What should be done differently next time?

Technology Development Process

Similar to policy development, technology development cannot be undertaken in a vacuum. All too often technology is developed in a lab and rushed to rapid implementation without consideration for the needs of the individuals in the working environment. The new technology may not have reached sufficient maturity to warrant deployment and it may even be in conflict with existing policies or already fielded technology. New technologies might take many years to emerge from laboratories and find its way into the field. As it pertains to electronic markets,

this rush negatively impacts the business value of the technical investment. Consequently, we propose developing new border security technology within the following framework.

The first phase of technology development involves the proof of concept, which requires building and testing a prototype system under laboratory conditions to determine if the proposed technology actually works. While the prototype is not intended to be scalable or full-featured, it is expected to have sufficient development to adequately model the final version in order to demonstrate the concept will work while gaining greater insight into the capabilities and limitations of the new technology.

The second phase of technology development is proof of value. This phase includes taking a revised prototype to the field and measuring whether the users are more productive with the system. In this phase the technology is placed in an operational field environment and operated by actual users. Far too often promising technology encounters unexpected difficulties in the field or even proves to be burdensome to the users. In this phase, it is important to measure and gauge the value afforded the users.

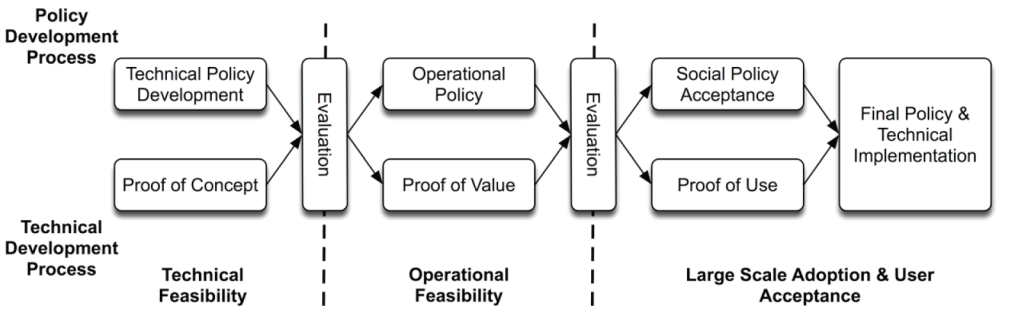
The final phase of technology development involves the proof of use. Typically this phase involves broad fielding and continued use by many users. In the case of border security, proof of use would equate to deployment of the technology across the border and finding that border security agents actually using the technology in support of border security. It is possible for technology to prove valid and useful, but not be widely accepted and used. Politics, newer technologies, or even lack of personal or organizational willpower can cause a proven technology to fail the proof of use phase. However, a collaborative process involving a network to follow-up through the process has been an effective way to ensure the usefulness of technologies (Dawes et al., 2009; Goldsmith & Eggers, 2004; Luna-Reyes et al., 2008)

Integrating Policy and Technology Development

Finally, policy and technology development cannot be developed independently. While each requires its own process as shown above, we believe the two processes should be integrated to ensure selected policy and technologies are compatible and implemented in an effective way that meets the stated goals (e.g., border security). Policy decisions must not prematurely rush under developed and unproven technology to the field and selected technology must meet stated policy goals. Only a coordinated effort between the two will allow policy and technology to improve border security and maximize the effectiveness of both. Figure 2 illustrates the close coordination required between the policy and technology development processes.

Under this model, results from technologies that have successfully passed the research laboratory proof of concept and field studies will serve as inputs into policy decisions, especially as those decisions relate to implementation plans. Policy decisions will then be based on

Figure 2. Policy – Technology integration model



empirical evidence, not simply interesting or fashionable technology and will translate into sound implementation decisions for the field. However, the process does not end there. Once an implementation decision has been made, proof of value will be evaluated. For technologies that demonstrate clear value, the technology will be continued through proof of use. Unsuccessful technologies will also then serve as new policy inputs and will guide future policy decision. We believe that marrying these two processes will ultimately result in a harmony between policy and technology implementation in support of collaborative border security. All this development needs to be understood as happening in a context of specific cross-border communities with local civic, political and economic interests (Brunet-Jailly, 2005). In fact, it is this particular network of actors who participate in the process of technology development, information and knowledge sharing (Navarrete et al., 2009).

POLICY RECOMMENDATIONS AND FUTURE RESEARCH

The importance of the US-Mexico border to both nations cannot be overstated. A smoothly operating border is critical to the economic propensity, domestic protection, and national security of both countries. The border is a milieu of competing interests in many different problem areas related to economic trade, health and the environment. Considering the problem area of economic flows (Brunet-Jailly, 2005), particularly the flows of people and products, maybe the most relevant competing interests are:

- Allowing access for lawful economic and immigration purposes;
- Securing the border against illegal activity.

Thus, one of the most challenging aspects of border operations is to distinguish criminals from economic-seeking expatriates, while at the same time limiting interference with legal and vital commerce. This can be most effectively accomplished via cross-national collaboration. Currently, there are gaps in both the technological infrastructure and international agreements, which limit the efficiency of border collaboration. This paper highlights the need for greater trust, better understanding of the current conditions on both sides of the border, innovative governance structures, effective leadership, interoperability and more effective information sharing between all parties. It also emphasizes the need for close coordination between border security policy and technology development.

From a process perspective, the ITAIDE project in the European Union is closely related to the Technology Integration Model and inter-organizational collaboration and governance ideas presented in previous sections of this paper. The ITAIDE project *Living Labs* are examples of networks of organizations working together to better understand their problems and create and test solutions and standards. Moreover, the design science approach appears to be an appropriate way of producing knowledge inside these inter-organizational networks. However, as in any other collaboration effort, it is very likely that different networks will have different levels of success, and it is still important to continue creating theories that contribute to more successful collaborations (Dawes, Cresswell & Pardo, 2009). Moreover, it is also important to consider that the ITAIDE project takes place in a very different context to the US-Mexico border.

In conclusion, we offer a brief list of concrete policy proposals, actions and next steps related to these border proposals:

1. To promote effective collaboration across the border, we believe that both countries need to promote an institutional design to analyze the border control problem and alternative solutions. A network of organizations appears to be an effective governance design to start working on this problem. Such a network should include representatives from the three levels of government, private organizations, uni-

versities and other non-profits interested in several aspects of border control, similar to the ITAIDE project. Although the effort could be initially started by an organization in either US or Mexico, we are convinced that the most effective governance design will lead to a shared responsibility by two main organizations, one on each side of the border;

2. We believe that the initial efforts of the network should be oriented to two main sets of activities. The first set of activities is related to developing working principles and to build legitimacy of the network. Other inter-organizational networks have developed such legitimacy on the basis of its formal inclusion in bi-national agreements as advisory boards, and through the collaborative development of bylaws in which they define the main rights and responsibilities of its members. The second set of activities is related to start developing a common understanding of the complexity of border control and security by identifying and characterizing its main problem areas. One problem area, for example, could be the asymmetrical situation in terms of information technology and systems infrastructure across the borders, or differences in incentives promoted by current legislation in both countries;
3. As mentioned in several parts of the paper, developing trust is crucial for the success of border security initiatives. In accordance with the frameworks presented in the paper, we believe that international agreements play an important role in providing some basis for collaboration (i.e., institutional trust). However, working together to develop projects and solve problems is the best way to build strong trust. In this way, the network may play again an important role in the trust building process, and choosing a problem or project in which is possible to show early positive results has been shown to be an effective way to accelerate the development of trust in many inter-organizational networks;
4. When technology plays a role in the development of potential solutions to specific problems, the prototyping approach that we described in Figure 2 has proven to be an effective way to either choose or develop the most appropriate technology for the problem situation. Moreover, the approach is effective to help participants to develop a shared understanding of the problem, and the intertwined interactions between policy, managerial and technical aspects of the solution;
5. Technical measures must be addressed to solve the heterogeneity of IT systems and information exchange across borders. Integrating disparate data is not a new problem or confined to cross-border information sharing. Well-known approaches and standards (e.g. XML, SOAP) should be applied to the border contexts in order to overcome the heterogeneous systems. The deployment of these types of technology should be married with development of appropriate information sharing policies. By applying well-known technical solutions and proactive policy, the sharing of data across borders could be overcome;
6. It is paramount that new border technologies be based on objective science and not on political currents or racial biases. The goal must be to facilitate border crossing, assist border personnel, and to limit subjective judgments and improper profiling. Any technologies that are developed must be examined and incorporated into existing screening decision processes and border constraints. We suggest following the methods and standards of the design science approach;
7. We propose that a border technology maturity model be developed as a standard means to evaluate cross-border security and information systems. The model would need to incorporate both technical and policy considerations and could be tied to the stages outlined in Figure 2. Technologies would be evaluated under both technical and policy lenses and both aspects

would have to be addressed to advance a technology in the maturity level. Technical maturity would be gauged based on the paradigm of "proof of concept", "proof of value", and "proof of use" as described above. Policy maturity would be based on the three steps defined above: problem to be solved, policy implementation, and policy evaluation. The maturity model could be used to assess current and planned technical solutions and would provide guidance for the industry. The model could also function as a decision tool for policy makers.

As pointed out in the paper, specific research on transnational technical infrastructures and collaboration is scarce. Such research is needed to better understand the complex relationships between our countries, and to align our goals and efforts to accomplish shared goals. The US and Mexico have a long, cherished, and important relationship. Improving trust and collaboration across all levels of border interaction, objectifying and improving border-screening technologies, and dramatically improving information sharing will ensure that this vital relationship remains strong, effective and seamless. The main actors of these collaboration efforts are public officials, but their actions need to be supported by research in areas related to the local culture of border regions and the interdependencies of our two nations in terms of the interchange of goods and people. It is likely that in the process we will need to redefine our concepts of sovereignty and our perception of people across the border.

REFERENCES

Ackleson, J. (2005). Border security technologies: Local and regional implications. *Review of Policy Research*, *22*(2), 137–155. doi:10.1111/j.1541-1338.2005.00126.x.

Ansell, C., & Gash, A. (2007). Collaborative governance in theory and practice. *Journal of Public Administration: Research and Theory*, *18*, 543–571. doi:10.1093/jopart/mum032.

Benítez Manaut, R., & Rodríguez Ulloa, C. (2006). Seguridad y Fronteras en Norteamérica. Del TLCAN a la ASPAN. *Frontera Norte*, *18*(035), 7–28.

Bertucci, G. (2006). Unlocking the human potential for public sector performance. *Public Personnel Management*, *35*(3), 175–179.

Bracchi, P., Cukic, B., & Cortellessa, V. (2006). Modeling the performance of border inspections with electronic travel documents. In *Proceedings of the 17th International Symposium on Software Reliability Engineering, 2006 (ISSRE '06)*.

Brunet-Jailly, E. (2005). Theorizing borders: An interdisciplinary perspective. *Geopolitics*, *10*(4), 633–649. doi:10.1080/14650040500318449.

Burgoon, J. K., Twitchell, D. P., Jensen, M. L., Meservy, T. O., Adkins, M., & Kruse, J. et al. (2009). Detecting concealment of intent in transportation screening: A proof of concept. *IEEE Transactions on Intelligent Transportation Systems*, *10*(1), 103–112. doi:10.1109/TITS.2008.2011700.

Carlile, P. (2002). A pragmatic view of knowledge and boundaries: Boundary objects in new product development. *Organization Science*, *13*(4), 442–455. doi:10.1287/orsc.13.4.442.2953.

CBP. T. S. (2009). Illegal immigration statistics. MIS Department, University of Arizona.

Cresswell, A. M., Burke, G. B., & Navarrete, C. (2009). *Mitigating cross-border air pollution: The power of a network.* Retrieved October 15, 2009, from http://www.ctg.albany.edu/publications/reports/jac_mitigating

Crosby, B., & Bryson, J. (2005). A leadership framework for cross-sector collaboration. *Public Management Review*, *7*(2), 177–201. doi:10.1080/14719030500090519.

Dawes, S. S., Cresswell, A. M., & Pardo, T. A. (2009). From "Need to Know" to "Need to Share": Tangled problems, information boundaries, and the building of public sector knowledge networks. *Public Administration Review*, *69*(3), 392–402. doi:10.1111/j.1540-6210.2009.01987_2.x.

Frederickson, H. G. (2005). Transcending the community: Local leadership in a world of shared power. *Public Management Review*, *87*(10), 8–15.

Gascó, M. (2004). E-Gobierno en Bolivia y Paraguay. In R. Araya Dujisin, & M. A. Porrúa Vigon (Eds.), *América Latina Puntogob: Casos y tendencias en gobierno electrónico* (pp. 125–150). Santiago: FLACSO-Chile/ AICD-OEA.

Goldsmith, S., & Eggers, W. D. (2004). *Governing by network: The new shape of the public sector*. Washington, DC: Brookings Institution Press.

Henningsson, S., Gal, U., Bjørn-Andersen, N., & Yao-Hua, T. (2011). The next generation information infrastructure for international trade. *Journal of Theoretical & Applied Electronic Commerce Research*, *6*(1), 1–15.

Henningsson, S., Rukanova, B., & Hrastinski, S. (2010). Resource dependencies in socio-technical information systems design research. *Communications of the Association for Information Systems*, *27*(1).

Kingsbury, N. (2002). *Border security: Challenges in implementing border technology: Statement of Nancy Kingsbury, Managing Director, Applied Research and Methods, before the Subcommittee on Terrorism, Technology, and Homeland Security and Subcommittee on Border Security, Immigration, and Citizenship, Committee on the Judiciary, United States Senate*. Washington, DC: U.S. General Accounting Office.

Livermore, C. R., & Rippa, P. (2011). ERP implementation across cultures: A political perspective. *International Journal of E-Politics*, *2*(4), 16–28. doi:10.4018/jep.2011100102.

Luna-Reyes, L. F., Black, L. J., Cresswell, A. M., & Pardo, T. A. (2008). Knowledge-sharing and trust in collaborative requirements analysis. *System Dynamics Review*, *24*(3), 265–297. doi:10.1002/sdr.404.

Luna-Reyes, L. F., Cresswell, A. M., & Richardson, G. P. (2004). Knowledge and the development of interpersonal trust: a dynamic model. In *Proceedings of the Hawiaiian International Conference on System Sciences-37*, HI.

Maldonado Carrasco, A. G. (2009). La Evolución de las Aduanas en México. *Comercio Exterior*, *59*(9), 746–753.

Navarrete, C., Mellouli, S., Pardo, T. A., & Gil-Garcia, J. R. (2009). Information sharing at national borders: Extending the utility of border theory. In *Proceedings of the Hawaiian International Conference on System Sciences-42,* HI.

Olson, G. (2010, 10/28/2010). Las armas se filtran por fisura en la Frontera con EU. *Excélsior*.

Pardo, T. A., Gil-Garcia, J. R., & Luna-Reyes, L. F. (2008). Collaborative governance and cross-boundary information sharing: Envisioning a networked and IT-enabled public administration. In *Proceedings of the Minnowbrook III.*

Perkins, K. L., & Placido, A. P. (2010). *U.S. Senate caucus on international narcotics control.* Washington DC. Retrieved July 12, 2012, from http://www.fbi.gov/news/testimony/drug-trafficking-violence-in-mexico-implications-for-the-united-states/

Raus, M., Liu, J., & Kipp, A. (2010). Evaluating IT innovations in a business-to-government context: A framework and its applications. *Government Information Quarterly*, *27*(2), 122. doi:10.1016/j.giq.2009.04.007.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, *23*(3), 393–404. doi:10.5465/AMR.1998.926617.

Rukanova, B., van Stijn, E., Henriksen, H. Z., Baida, Z., & Yao-Hua, T. (2009). Understanding the influence of multiple levels of governments on the development of inter-organizational systems. *European Journal of Information Systems*, *18*(5), 387–408. doi:10.1057/ejis.2009.28.

Secretaría de Hacienda y Crédito Público. (2007). *Plan de Modernización de Aduanas 2007-2012*.

Tan, Y. H., Bjorn-Andersen, N., & Henningsson, S. (2010). Developing an information infrastructure for international trade. In *Proceedings of the AMCIS2010.*

Tsiamyrtzis, P., Dowdall, J., Shastri, D., Pavlidis, I., Frank, M., & Ekman, P. (2007). Imaging facial physiology for the detection of deceit. *International Journal of Computer Vision*, *71*(2), 197–214. doi:10.1007/s11263-006-6106-y.

Velázquez García, M. A. (2008). La Construcción de la Imagen de México en Estados Unidos desde una Perspectiva de Riesgo. *Frontera Norte*, *20*(039), 37–67.

Vogel, T., Schmidt, A., Lemm, A., & Österle, H. (2008). Service and document based interoperability for European ecustoms solutions. *Journal of Theoretical & Applied Electronic Commerce Research*, *3*(3), 17–36.

Washburn, R. S. (2004). Globalization, territorialized economic development and power plants on the U.S.-Mexico border. In *Proceedings of the Annual Meeting of the American Sociological Association,* San Francisco, CA.

Wein, L. M., & Baveja, M. (2005). Using fingerprint image quality to improve the identification performance of the U.S. Visitor and immigrant status indicator technology program. *Proceedings of the National Academy of Sciences of the United States of America*, *102*(21), 7772–7775. doi:10.1073/pnas.0407496102 PMID:15894628.

ENDNOTES

1 Article 11 of the Mexican Constitution gives Mexican citizens the right of entering or leaving the Republic, traveling through its territory and change place of residency without the need of a Laissez-passer, Passport or other similar requirements. This individual right is subordinated to judicial authorities in cases of criminal activities and to administrative authorities on the basis of limitations imposed by, for example, health or migration laws.

Luis Felipe Luna-Reyes is a Professor of Business at the Universidad de las Américas Puebla in Mexico. He holds a Ph.D. in Information Science from the University at Albany. Luna-Reyes is also a member of the Mexican National Research System. His research focuses on electronic government and modeling collaboration processes in the development of information technologies across functional and organizational boundaries.

Douglas C. Derrick is an Assistant Professor of IT Innovation at the University of Nebraska at Omaha and received his PhD in Management Information Systems from the University of Arizona. He holds a Masters degree in Computer Science from Texas A&M University and a Masters degree in Business of Administration from San Jose State University. He is a Distinguished Graduate from the United States Air Force Academy. His research interests include human-computer interactions, intelligent agents, data fusion, decision support systems, and persuasive technology

Brent T. Langhals is an active duty Air Force Lieutenant Colonel and is currently appointed as Assistant Professor of Engineering Systems at the Air Force Institute of Technology, Wright-Patterson AFB, OH. Dr Langhals received his PhD in Management Information Systems from the University of Arizona in 2012. His research interests include vigilance, human-systems interaction, and border security.

Jay F. Nunamaker, Jr. is Regents and Soldwedel Professor of MIS, Computer Science and Communication. He is Director of the Center for the Management of Information and the National Center for Border Security and Immigration at the University of Arizona. Dr. Nunamaker was inducted into the Design Science Hall of Fame, May 2008. Dr. Nunamaker received the LEO Award for Lifetime Achievement from the Association of Information Systems (AIS) at ICIS in Barcelona, Spain, December 2002. He was elected a fellow of the AIS in 2000. He is widely published with an H index of 53 in the fields of collaboration technology and deception detection. Dr. Nunamaker received his Ph.D. in operations research and systems engineering from Case Institute of Technology.