Information Sharing in the Regulatory Context: Revisiting the Concepts of Cross-Boundary Information Sharing

J. Ramon Gil-Garcia

Center for Technology in Government
University at Albany
187 Wolf Road Suite 301
Albany NY 12205

jgil-garcia@ctg.albany.edu

Theresa A. Pardo

Center for Technology in Government
University at Albany
187 Wolf Road Suite 301
Albany NY 12205

tpardo@ctg.albany.edu

Megan K. Sutherland

Center for Technology in Government
University at Albany
187 Wolf Road Suite 301
Albany NY 12205

msutherland@ctg.albany.edu

ABSTRACT

Cross-Boundary Information Sharing (CBIS) has become increasingly important for public and private sector entities around the world. Studies critical to advancing what is known, have focused primarily on information sharing and integration among government entities at the same level of government or between governments from different levels. Within the context of government regulation, information sharing typically occurs among a more diverse network of actors and processes with overlapping regulatory responsibilities and information needs. The variety of actors and overlapping regulatory relationships can contribute to a gap between the level and nature of information sharing required for individual actors to meet their obligations. This ongoing research paper looks at the socio-technical nature of information sharing among public and private sector actors and examines what is known about public-public and private-private CBIS sector in order to inform future research..

CCS Concepts

• Applied computing~E-government

Keywords

Private Sector; Public Sector; Information Sharing; Standards; Incentives; Trusted Networks; Integrated Data; Interoperability; Public-private Partnerships; Regulation; Cross-Boundary Information Sharing

1. INTRODUCTION

Financial market regulation (FMR) in the U.S. has transformed to meet today's fast-paced, innovation-driven, inter-dependent and complex market needs. The recent global economic crisis tells us that more attention is needed to this critical governmental responsibility. According to Mary Shapiro, Chair of the U.S. Securities and Exchange Commission at the beginning of the economic crisis in 2007, new attention must be paid to information sharing in FMR. Government and private sector regulators depend on information to monitor market activity in order to do their jobs. They use information to mitigate risk and stabilize markets while

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

ICEGOV '15-16, March 01 - 03, 2016, Montevideo, Uruguay
Copyright is held by the owner/author(s). Publication rights licensed to ACM.
ACM 978-1-4503-3640-6/16/03...\$15.00
DOI: <http://dx.doi.org/10.1145/2910019.2910099>

private industry relies on information to stay competitive and compliant. However, sharing financial market information across networks comprised of both public and private sector entities requires balance to ensure market and trading system stability while also maintaining the privacy and security needs of private industry.

Regulatory relationships, such as those found in FMR, are based primarily on compliance in which regulatory agencies require information from industry in order to monitor and control aspects of that industry. Of particular interest are the asymmetric relationships that occur among actors in the context of FMR. The hierarchical relationships that occur across the public and private sector in this context influence the nature of CBIS and decisions related to fit between CBIS in this context with known types and components of information sharing. In this context, CBIS among public and private entities requires additional study.

Cross-boundary information sharing (CBIS), regardless of the context within which it occurs, involves a set of diverse actors and processes with overlapping responsibilities and information needs forming a complex network of relationships and actions. Research into the complex nature of CBIS when the sharing partners are within the private sector is limited. Even less research which examines sharing relationships between public and private sector entities, such as the case of FMR, is available.

Understanding the various components and Information Sharing (IS) types within regulatory environments such as the food industry, environmental regulation or FMR is still fairly new to the research community. Much current understanding of CBIS lies within the public sector. In the private sector, studies on CBIS within the private sector have focused heavily on supply chains.

As a complement to existing studies, this ongoing research paper takes a socio-technical approach and examines the various similarities and differences between the dimensions and challenges of Cross-Boundary Information Sharing (CBIS) when looking at the relationships and activities that occur in public-public, private-private and public-private relationships in order to better identify research areas looking at IS in the regulatory environment. This research will draw on nuances between the public and private sector CBIS to assist in defining and characterizing the complex relationships that occur among public and private sector actors and activities to support future studies in CBIS in critical areas such as FMR and food traceability.

This paper is organized in four sections, including the foregoing introduction. Section two provides a brief literature review and highlights a few key concepts from the public and private sector as well as from IS relationships present in public-private partnerships. Section three addresses the common themes and differences seen among the public and private sector CBIS relationships and activities. Section four presents some next steps for looking at CBIS

in the regulatory environment, in which public and private entities are compelled to exchange information and how CBIS affects regulatory relationships, activities, and outcomes.

2. LITERATURE REVIEW

Research on the concept of CBIS and integration has been approached from the technical, social and organizational perspectives and through the lenses of many policy domains. Studies using a technical perspective have examined issues such as data standards and the technical infrastructure necessary for sharing. Such studies include evaluations of the technical obstacles to sharing across multiple platforms and diverse data structures and designs [1]. Studies conducted with a social or organizational perspective include examinations of trust among participants and incentives. Such studies included examinations of the social, business and organizational factors that contribute to the capability of an organization to share information across internal and external boundaries [2]. Results of these studies consistently conclude that sharing information across boundaries involves complex interactions among technical, social and organizational processes [3] and can be seen understood as a socio-technical phenomenon.

To lay the foundation for building new understanding of CBIS in the regulatory environment it is necessary to look at literature focused in both the public sector and the private sector. While studies with a focus on CBIS in the public sector are numerous, studies focused on CBIS in the private sector were difficult to find. Those that were discoverable focused primarily on IS within the context of a supply chain. Therefore in this preliminary literature we look to these studies to provide insight into current understanding of the sharing of information in the private sector, with the supply chain as the primary context.

2.1 Cross-Boundary Information Sharing

Scholars and practitioners have proposed numerous classification schemes for IS and integration in the public sector. Most of this work has focused on IS among government agencies at the same level of government or between government agencies from different levels of government, i.e. national and sub-national [4, 5, 6, 7, 8]. Many of these studies and initiatives have looked at intra-organizational, inter-organizational and intergovernmental IS through the context of government information. For example, Tung-Mou Yan and Terrence Maxwell [9] highlight interpersonal IS, which looks at an individual's behavior such as motivation that impacts an individual's willingness to share information.

Gil-Garcia and his colleagues [10] propose a framework on IS in the public sector. The first dimension of this framework focuses on purpose of the sharing which can be (1) meeting a specific need or addressing a specific problem or (2) building systemic capacity for the organizations involved. In some cases, IS is needed in order to solve a specific public problem or meet a societal need. For example, CBIS initiatives in the domain of criminal justice are typically undertaken to share and integrate data that will help agencies to inform, support, and execute coordinated planning and response activities.

The second dimension of the framework [10] refers to the nature of the relationship among organizations involved in an IS activity, which could be (1) intra-organizational; (2) inter-organizational; and intergovernmental. In the public sector, the intra-organizational category comprises IS across multiple units or areas within a single government entity. Inter-organizational initiatives would normally include IS across governmental units from the same level of government. Finally, intergovernmental characterizes IS initiatives

that take place across organizations from different levels of government, i.e. national and local.

Looking at cross-boundary IS in the private sector provides an opportunity to assess similarities and differences with public sector CBIS. The flow of shared information within a supply chain generally flows in upstream and downstream directions [11]. IS is necessary across entities in a supply chain in this way for various purposes, such as investment or managing operations and so that decisions throughout the supply chain can be conducted in a coordinated way [12]. Within the context of supply chains, there are similar CBIS classifications schemes to the Gil-Garcia Framework, including IS with suppliers; internal IS (within the organization); and IS with customers [13]. To support IS within the supply chain, Hau Lee and Seungjin Whang [12] describe three IS models including the information transfer model (information transferred from one partner to the other who then maintains that information for decision-making); the third party model (third party who collects information and maintains it in a database for the supply chain); and finally the information hub model (similar to third party model but instead of a third party, there is a system in place that maintains a database) [12].

2.2 Components of CBIS

Understanding CBIS as a socio-technical phenomenon requires the consideration of four components [14]: trusted social networks (social actors who know and trust one another); shared information (sharing of knowledge both formal and informal); integrated data (integration of data at the level of data element standards or industry/community standards); and interoperable technical infrastructure (systems that can communicate with one another at the hardware/operating system level).

Trusted social networks, as the first component of understanding CBIS as a socio-technical phenomenon, characterize an array of both formal and informal relationships among organizations and individuals and across policy domains, in which trust enables the nature of IS relationships these trusted social networks are very important for enabling not only IS but standards, and interoperable technical infrastructure as well as collaboration among organizations and individuals [14, 15].

According to the literature that draws on private sector studies, trust is among one of the most recognized components of IS along the supply chain. Trust, as defined by Hopp presents a continuum with extremes of complete trust and complete distrust in order to identify trustworthiness, which is measured by credibility as well as competence and social characteristics [16]. Capaldo defines trust as the expected collaboration in which the expectation is that partners will do what is best for the entire system, even when that may lead to a partner's disadvantage [17]. Trust and other social aspects such as willingness and motivation, are important at both the individual and the organizational level of IS within the supply chain and in other contexts such as collaborative products and system design [18]. These individual behaviors can affect activity in both the public and private sector. In the private sector, for instance, trust can impact supply chain activity as well as relationships between salespeople, manufacturers and other actors within the supply chain [16]. Moreover, without trust, supply chain partners are less likely to collaborate in a way that positively affects the system as a whole [17]. Among trust, the activities, models and relationships that support supply chain IS also require timeliness and accuracy in order for sharing to be effective [12].

In the context of public-private partnerships, lack of trust is closely tied to poor IS and failed communication [19]. Public-private

partnerships that exist between government and private industry represent heterogeneous teams of public and private actors that have varying values and objectives [20]. Crowther redefines IS to fit the context of public-private partnerships by stating that IS is the “common stewardship of information through the acts of partnering, dissemination, and fusion, with the objectives of shared understanding, consistent decision-making, and coordinated action to achieve collaborative goals” [21].

Shared information, as the second component of CBIS as a socio-technical phenomenon, relates to two very important concepts: IS and information integration. While these concepts linked, they are also quite distinct. IS refers to the actual exchange of information and knowledge across organizational boundaries and has little to do with the media through which sharing occurs. Together, trusted social networks and shared information represent the social components of information integration [14].

CBIS across sectors can include different types of information. Tung-Mou Yang and Yi-Jung Wu discuss five types of shared information including: collected raw data (data directly or indirectly collected for regular government operations); value-added information (raw data further analyzed and refined); administration oriented information (information of government documents, meetings, activities); domain-oriented information (core-business knowledge of government agency); and administration oriented knowledge (general knowledge of government daily administrative operations) [22]. These types of shared information can be characterized as 1) privacy or confidentiality related information, or 2) public safety related information or 3) public information [22].

Shared information within supply chains includes sales data, inventory information, order statuses, and product/delivery schedules [12, 16]. There are other types of shared information including information on performance metrics and capacity [12]. These types of information are shared for the purpose of maintaining operations, measuring performance, manage product delivery and so on [11]. Different activities can involve various actors throughout the supply chain and information can be shared between different partners in either the upstream or the downstream flow of information. For instance, a manufacturer may share information on forecasting and production planning with its suppliers. In turn, a supplier may share inventory or capacity information with the manufacturer [13].

Data integration, as the third component of understanding CBIS as a socio-technical phenomenon, can be described as “integration of data at the level of data element standards and/or industry/community data standards” [14]. Integration is not only complex, but multidimensional including factors related to technology but also organizational, political, economic, institutional and social components that can impact capability to integrate data [4]. The impact of these factors can vary greatly depending on the context and nature of the sharing relationships, the types of information and the degree of integration sought.

Interoperable technical infrastructure, as the fourth component of understanding CBIS as a socio-technical phenomenon, refers to systems that have the capability to communicate with other systems at the hardware/operating system level. Interoperability allows multiple entities to share information using similar standards and potentially the same infrastructure [23]. Such interoperability relies on robust and reliable intra and internet functionality and often comprises, not a single system, but a “system of systems” [14]. For private sector firms in the FMR context, technology to support data

integration and interoperable infrastructure changes rapidly. While private firms may have the resources to adapt to these changes; government regulatory entities are challenged to keep pace with emerging technologies, new trading models and methods.

3. CBIS IN THE PUBLIC AND PRIVATE SECTOR

The preceding section laid the foundation for a preliminary analysis CBIS in the public and in the private sector. While the analysis is not complete, it highlights a number of salient points for discussion and which serve as a formal foundation for advancing understanding of CBIS in the regulatory context.

Both sectors see trust as a necessary component to maintain strong relationships among sharing partners [12, 16]. Moreover it is apparent that shared information, interoperability, and technical infrastructure are important to both public and private sector efforts to protect privacy, and mitigate risk [18, 21, 24]. Despite these similarities, there are gaps in what is known about IS where sharing relationships cross public-private sector bounds.

Supply chains offer insight into types of information shared and components of trust and how those impact CBIS capability. Standards, data accuracy and timely communication, as part of internal information integration, are important to supply chain IS [13], but there doesn't appear to be as much high-level research of how these change across supply chains and what activities impact timeliness and data accuracy of such IS efforts.

In trying to address CBIS in the regulatory context, it is important to keep in mind the similarities and differences between the private and public sector. While supply chain and public sector IS are similar in some regards, Donald Kettl sees the driving force behind the private sector as competition and the economy of operations while in the public sector, the pressures of competition are few, if any [25]. This driving force changes the way information is shared and how components of IS, such as trust, are viewed by public and private sector sharing partners. The nuances of CBIS between public and private sharing partners are not well known, nor is there much known about how such nuances impact IS in the regulatory context. The research in progress paper is a step in closing this knowledge gap.

The challenges seen in the CBIS relationships in public-private partnerships including challenges of trust, information overload, and low quality information are challenges that are shared in areas like FMR, public health and human services. These challenges are not mutually exclusive and include issues of disclosure, proprietary information, and security of trade-secret information and so forth [24]. For public and private sector entities to work together and share information new understanding of each partner's IS capability is required [26]. Furthermore, there is a need to better understand the value and risk associated with certain types of information shared for specific purposes. For instance, trade-secret data shared with hundreds of people may be information that is deemed less valuable than information shared with a smaller, more select group of people [24].

4. MOVING FORWARD

Moving forward it is important to keep in mind the nature of the regulatory environment which is multi-sector and hierarchical. In this sense, unlike relationships that are public-public or private-private, regulatory relationships require private-public ties that are not ‘partnerships’ in the way public-private partnerships within emergency management or public safety exist. To better understand

how multi-sectoral and hierarchal relationships impact CBIS in the regulatory environment, we need better understanding of the nuances of data integration, and interoperable technical infrastructure across and within firms. Moreover, we need to further explore the nature of trust in public-private relationships and the implications of trust in this context has on our understanding of CBIS, particularly in situations in which reporting is mandatory.

5. REFERENCES

- [1] Pardo, T. A., Gil-Garcia, J. R., & Burke, G. B. (2006). Building response capacity through cross-boundary information sharing: The critical role of trust. *Exploiting the Knowledge Economy: Issues, Applications, Case Studies*.
- [2] Pardo, T. A., Gil-García, J. R., & Burke, G. B. (2009). Information sharing and public health: A case-based look at the ICT expectations-reality gap. *ICTs, citizens and governance: After the hype*, 180-197.
- [3] Pardo, T. A., Gil-Garcia, J. R., & Burke, G. B. (2008). Sustainable cross-boundary information sharing. In *Digital Government* (pp. 421-438). Springer US.
- [4] Gil-Garcia, J. R. (2012). Towards a smart State? Inter-agency collaboration, information integration, and beyond. *Information Polity*, 17(3), 269-280.
- [5] Luna-Reyes, L. F., & Gil-Garcia, J. R. (2014). Digital government transformation and internet portals: The co-evolution of technology, organizations, and institutions. *Government Information Quarterly*, 31(4), 545-555.
- [6] Gil-Garcia, J. R., Chun, S. A., & Janssen, M. (2009). Government information sharing and integration: Combining the social and the technical. *Information Polity*, 14(1), 1-10.
- [7] Luna-Reyes, L. F., Gil-Garcia, J. R., & Estrada-Marroquin, M. (2008). The impact of institutions on interorganizational IT projects in the Mexican federal government. *International Journal of Electronic Government Research*, 4(2), 27-42.
- [8] Luna-Reyes, L. F., Gil-Garcia, J. R., & Cruz, C. B. (2007). Collaborative digital government in Mexico: Some lessons from federal Web-based interorganizational information integration initiatives. *Government Information Quarterly*, 24(4), 808-826.
- [9] Yang, T. M., & Maxwell, T. A. (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly*, 28(2), 164-175.
- [10] Gil-Garcia, J. R., Schneider, C. A., Pardo, T. A., & Cresswell, A. M. (2005). Interorganizational information integration in the criminal justice enterprise: Preliminary lessons from state and county initiatives. In *System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on* (pp. 118c-118c). IEEE.
- [11] Costantino, F. M. (2015). The impact of information sharing on ordering policies to improve supply chain performances. *Computers & Industrial Engineering*, 82127-142.
- [12] Lee, H. L., & Whang, S. (2000). Information sharing in a supply chain. *International Journal of Manufacturing Technology and Management*, 1(1), 79-93.
- [13] Huo, B., Zhao, X., & Zhou, H. (2014). The Effects of Competitive Environment on Supply Chain Information Sharing and Performance: An Empirical Study in China. *Production & Operations Management*, 23(4), 552-569.
- [14] Gil-Garcia, J., Pardo, T., & Burke, G. (2010). Conceptualizing information integration in government. *Advances of Management Information Systems*, 17, 179.
- [15] Luna-Reyes, L. F., Gil-Garcia, J. R., & Cruz, C. B. (2007). Collaborative digital government in Mexico: Some lessons from federal Web-based interorganizational information integration initiatives. *Government Information Quarterly*, 24(4), 808-826.
- [16] Ebrahim-Khanjari, N., Hopp, W., & Iravani, S. R. (2012). Trust and Information Sharing in Supply Chains. *Production & Operations Management*, 21(3), 444-464.
- [17] Capaldo, A., & Giannoccaro, I. (2015). How does trust affect performance in the supply chain? The moderating role of interdependence. *International Journal of Production Economics*, 16636-49.
- [18] Jarvenpaa, S. L., & Staples, D. S. (2000). The use of collaborative electronic media for information sharing: an exploratory study of determinants. *The Journal of Strategic Information Systems*, 9(2), 129-154.
- [19] Givens, A. D., & Busch, N. E. (2013). Information Sharing and Public-Private Partnerships: The Impact on Homeland Security. *Homeland Security Review*, 7(2), 123-150.
- [20] Nissen, H. A., Evald, M. R., & Clarke, A. H. (2014). Knowledge sharing in heterogeneous teams through collaboration and cooperation: Exemplified through Public-Private-Innovation partnerships. *Industrial Marketing Management*, 43(Special Issue on Innovation in Networks - Per Freytag and Louise Young), 473-482.
- [21] Crowther, K. G. (2014). Understanding and Overcoming Information Sharing Failures. *Journal of Homeland Security & Emergency Management*, 11(1), 131-154.
- [22] Tung-Mou, Y., & Yi-Jung, W. (2013). What to Share and Why to Share? A Case Study of Cross- Boundary Information Sharing in Taiwan e-Government. *Journal of Library & Information Studies*, 11(1), 25-53.
- [23] Pardo, T. A., Gil-Garcia, J. R., & Luna-Reyes, L. F. (2010). Collaborative governance and cross-boundary information sharing: envisioning a networked and IT-enabled public administration. *The future of public administration around the world: The Minnowbrook Perspective*, 129-39.
- [24] Morris, B. W., Kleist, V. F., Dull, R. B., & Tanner, C. D. (2014). Secure Information Market: A Model to Support Information Sharing, Data Fusion, Privacy, and Decisions. *Journal of Information Systems*, 28(1), 269-285.
- [25] Kettl, D. F. (1993). *Sharing power: Public governance and private markets*. Brookings Institution Press.
- [26] Sayogo, D. S., Pardo, T. A., & Bloniarz, P. (2012). Information sharing and financial market regulation: understanding the capability gap. *Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance* (pp. 123-131). ACM.