6-2014

Data Sharing Issues and Potential Solutions for Adoption of Information Infrastructures: Evidence from a Data Pipeline Project in the Global Supply Chain over Sea

Arjan Knol
Delft University of Technology, the Netherlands, a.j.knol@tudelft.nl

Bram Klievink
Delft University of Technology, the Netherlands, a.j.klievink@tudelft.nl

Yao-hua Tan
Delft University of Technology, the Netherlands, y.tan@tudelft.nl

27th Bled eConference

eEcosystems

June 1 - 5, 2014; Bled, Slovenia

Data Sharing Issues and Potential Solutions for Adoption of Information Infrastructures: *Evidence from a Data Pipeline Project in the Global Supply Chain over Sea*

Arjan Knol

Delft University of Technology, the Netherlands

a.j.knol@tudelft.nl

Bram Klievink

Delft University of Technology, the Netherlands

a.j.klievink@tudelft.nl

Yao-hua Tan

Delft University of Technology, the Netherlands

y.tan@tudelft.nl

Abstract

Information infrastructures have gained significant momentum in today's information economy. They are defined as shared, open and evolving socio-technical systems providing distinct IT capabilities. The Cassandra EU project aims to enhance visibility of the international flow of goods over sea with an electronic data pipeline as an information infrastructure. This paper presents data sharing issues that could prevent adoption of the Cassandra Pipeline. Potential solutions are provided regarding access restriction and data sharing. In addition solutions are derived from the design theory for dynamic complexity in information infrastructures of Hanseth and Lyytinen (2010), proposing to gain momentum by starting small, focusing on immediate benefits for supply chain partners and obtaining experience using simple prototypes. This paper underlines that designers of the Cassandra Pipeline as an information infrastructure need to think carefully about the implications of restricting access and non-obligatory or obligatory data sharing, both allowing for generativity and trust while preventing potential abuse at the same time.

Keywords: Information Infrastructures, Digital Infrastructures, Digital Eco Systems, Issues, Adoption, Design Science, Design Theory, Supply Chain Management

1 Introduction

In today's information economy the notion of *information infrastructures* has gained significant momentum. An information infrastructure (or digital infrastructure or digital eco system) is defined as "a shared, open, heterogeneous and evolving socio-technical system of Information Technology (IT) capabilities" (Hanseth and Lyytinen, 2010, p1). Information infrastructures vary in scale, functionality and scope as clarified by examples such as the Internet, Electronic Data Interchange (EDI) networks, electronic market places such as eBay, operating systems such as Windows and Linux, Apple's iTunes store, Google's Play store, NetFlix or Spotify (Hanseth and Lyytinen, 2010; Janssen et al., 2009; Tilson et al., 2010). Information infrastructures are built on the notion of generativity which is "an ability or capacity to generate or produce something" (Avital and Te'Eni, 2009, p347). Catering to generativity, information infrastructures are shared and open systems that continuously evolve over time, trusting members to invent and share new uses along the way (Tilson et al., 2010). "An essential characteristic of infrastructures is that they are used by many different users, with the usage evolving over time, as may the type of users" (Janssen et al., 2009, p233). Hence, designers of open, shared and evolving information infrastructures need to trust users to self-organise and invent new capabilities along the way, essentially embracing bottom-up experimental design in a socio-technical context using distributed and loosely-coupled control mechanisms (Hanseth and Lyytinen, 2010).

Effectively designed information infrastructures can be highly beneficial for individuals, organisations and societies as shown by aforementioned infrastructure examples such as the Internet, yet achieving success is easier said than done and many design initiatives fail to deliver expected benefits (Hanseth and Lyytinen, 2010). Achieving generativity within shared, open and evolving information infrastructures seems a complex matter for designers who need to embrace bottom-up change in a socio-technical context and distance themselves from traditional top-down design approaches in which systems could be defined through a distinct set of functional requirements within strict boundaries (Tilson et al., 2010). For example Hanseth and Lyytinen (2010) mention difficulties for designers in persuading users to adopt information infrastructures while the user community is still small (the so-called *bootstrap problem)* as well as difficulties to adapt to increasingly varying needs once growing (the so-called adaptability problem). Hence, overall it seems that effectively designing information infrastructures that evolve over time and in which data is generated and shared by users seems easier said than done.

This paper presents data sharing issues and potential solutions for adoption of information infrastructures that are derived from a European Union (EU) project called Cassandra which aims to enhance supply chain visibility of global sea cargo with an electronic data pipeline. As explained in further detail later, the Cassandra Pipeline concept can be seen as an information infrastructure in the making in that it proposes a shared socio-technical system for enhancement of global supply chain visibility over sea that evolves over time using distributed and loosely-coupled control mechanisms.

The issues presented in this paper revolve around difficulties for designers to persuade groups of users to adopt the Cassandra Pipeline as an information infrastructure in the making. As such this paper is of academic relevance in that it provides confirmatory case study material regarding Hanseth and Lyytinen's (2010) bootstrap problem.

Moreover potential solutions regarding data access and data sharing are discussed, linking back to Hanseth and Lyytinen's (2010) design theory for dynamic complexity in information infrastructures. This paper is of practical relevance for designers of information infrastructures in that it provides examples of data sharing issues as well as potential solutions for adoption.

2 Background

This section provides background information regarding the Cassandra Pipeline project and the design theory for dynamic complexity in information infrastructures.

2.1 The Cassandra Pipeline: an Information Infrastructure

Cassandra stands for "common assessment and analysis of risk in global supply chains" (Cassandra-project.eu)[1]. The EU project is composed of 26 partners ranging from research institutes to global supply chain industry partners to governments. The Cassandra project introduces an electronic data pipeline as a data sharing concept to ensure control and security in the international flow of containerised cargo over sea. The Cassandra Pipeline aims to increase international supply chain data quality by obtaining data from the source enabling both governments and businesses to conduct higher quality risk analyses. The business domain can for example improve its decision-making by predicting "optimal" transport modes based on timely and accurate data (the synchro-modality concept, Klievink et al., 2012) whereas the governmental domain can reap benefits by re-using business source data for customs control purposes (the piggy-backing concept of Tan et al., 2011). Figure 1 provides an overview of the Cassandra Pipeline concept.

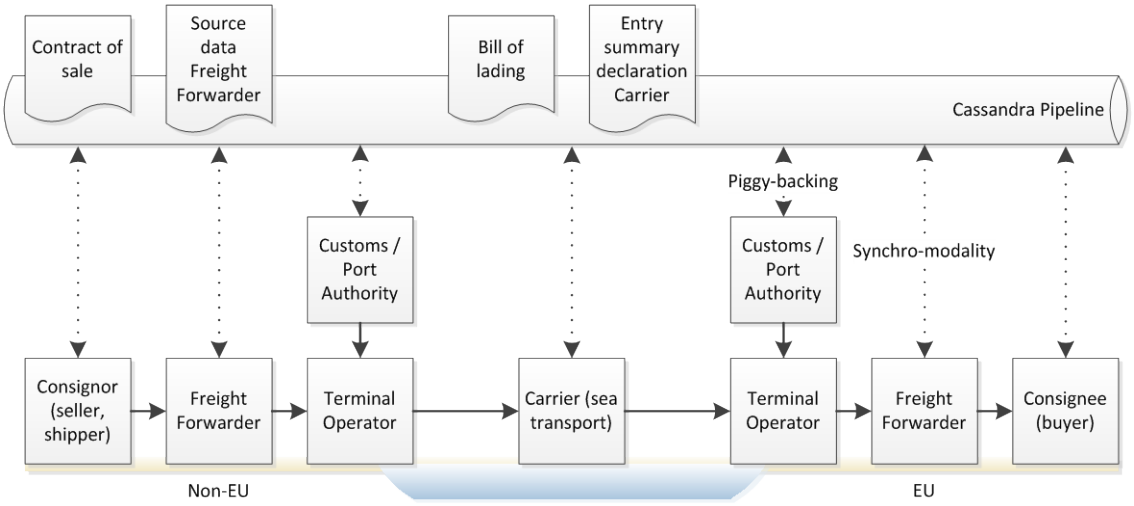

Figure 1: The Cassandra Pipeline concept providing data from the source and connecting key supply chain partners to enhance supply chain visibility of the global supply chain over sea

1 In Greek mythology a woman named Cassandra was given the power to predict the future by the God Apollo who wanted to seduce her. Since she refused his seduction Apollo punished her with a curse of never being believed. The so-called Cassandra syndrome refers to predictions that are not commonly believed at first yet will come true at some point, possibly clarifying the ambitions of the Cassandra Pipeline concept (Wikipedia.org, 2013).

The Cassandra Pipeline concept essentially encompasses the design of an information infrastructure because the concept proposes (Hanseth and Lyytinen, 2010):

- *Sharing* among a growing number of user communities, designers and regulators (generativity);
- *Openness* in that any new IT capability, designer or user community can be added as long as it conforms to the architectural principles regarding data sharing among the pipeline (unboundedness);
- *Heterogeneity* referring to an increase in diversity over time both socially and technically;
- *Evolution* in that it aims to continuously evolve, unlimited by time or user community;
- *Distinct IT capabilities* that are designed, implemented and maintained by designers and users;
- *Distributed and loosely-coupled control mechanisms* among a large set of designers and users.

2.2 Design Theory for Dynamic Complexity in Information Infrastructures

A design theory essentially proposes "how to do something" (Gregor and Jones, 2007, p313). The design theory for dynamic complexity in information infrastructures of Hanseth and Lyytinen (2010) draws upon the Complex Adaptive Systems theory which investigates how self-organising systems adapt and evolve (Benbya and McKelvey, 2006; Holland, 2006). The design theory aims to: "(1) create an attractor that feeds system growth to address the bootstrap problem; and: (2) assure that the emerging system will remain adaptable at 'the edge of chaos' while it grows to address the adaptability problem" (Hanseth and Lyytinen, 2010, p6). In other words, the theory proposes directions in how to achieve momentum and how to allow for adaptability when designing information infrastructures. Three design principles and twelve corresponding design rules for tackling bootstrap problems are provided:

1. Design initially for usefulness:
    - DR1. Target IT capability to a small group;
    - DR2. Make IT capability directly useful without an installed base;
    - DR3. Make IT capability simple to use and implement;
    - DR4. Design for one-to-many IT capabilities in contrast to all-to-all.
2. Build upon existing installed bases:
    - DR5. Design IT capability that does not depend on new support infrastructure;
    - DR6. Deploy existing transport infrastructures;
    - DR7. Build gateways to existing service and application infrastructures;
    - DR8. Use bandwagons associated with other information infrastructures.
3. Expand installed base by persuasive tactics to gain momentum
    - DR9. Users before functionality;
    - DR10. Enhance the IT capability within the information infrastructure only when needed;
    - DR11. Build and align incentives as needed;
    - DR12. Develop support communities.

3 Approach

This research project overall aims to 1) identify issues that could prevent adoption of information infrastructures and 2) design and evaluate corresponding solutions. To achieve this objective this research uses design science of Hevner and Chatterjee (2010) as a research philosophy effectuated with the inductive-hypothetic research strategy of Sol (1982). Accordingly, this research starts with identification of issues from practice that could prevent adoption of information infrastructures and hereafter continues with design and evaluation of corresponding solutions. These solutions are called artefacts that are either constructs, models, methods or instantiations (March and Smith, 1995; Winter, 2008). Four main research phases are identified following an inductive reasoning process:

1. *Exploration:* description of an empirical situation;
2. *Understanding:* abstraction of essential aspects in a conceptual model;
3. *Design:* theory formulation resulting in the creation and implementation of an artefact;
4. *Evaluation:* evaluation (validation) of the artefact.

This paper presents results from the exploration and understanding research phases by presenting issues that are derived from the Cassandra Pipeline project (related to the bootstrap problem of Hanseth and Lyytinen, 2010). The issues are derived from internal project documentation analysis as well as project meetings and project publications. In addition this paper presents potential data sharing solutions linking back to Hanseth and Lyytinen's (2010) design theory for dynamic complexity in information infrastructures[2]. Further identification of issues and design and evaluation of solutions are next steps and therefore recommended for future research.

Hanseth and Lyytinen (2010) applied their design theory to the Internet case study, among others providing a table in which their design principles and design rules are linked to evidence from the Internet design history. In this paper the design theory is applied to the Cassandra Pipeline case study. In terms of openness and control the Cassandra Pipeline information infrastructure differs from the Internet case. The Internet is developed as a loosely-controlled and open information infrastructure whereas the Cassandra Pipeline is developed as a tightly-controlled and restricted open information infrastructure. This acknowledged difference makes investigation whether design principles and rules of Hanseth and Lyytinen (2010) can be applied to the Cassandra Pipeline case an interesting endeavour.

4 Data Sharing Issues

This section provides data sharing issues that can prevent future adoption of the Cassandra Pipeline concept.

4.1 Issue 1: Changing Liability

In the international supply chain goods are sold by sellers (consignors) to buyers (consignees) using a contract of sale. Consignors delegate container transport over sea

2 Hanseth and Lyytinen's (2010) design theory is also applied by Aanestad and Jensen (2011) in the healthcare domain. This paper applies the design theory to the supply chain domain.

to carriers who ensure that goods are delivered to consignees. To acknowledge that the goods have been received for carriage, the carrier issues a transport document to the consignor called the bill of lading for sea cargo. Based on data on the bill of lading carriers also send digital Entry Summary Declarations (ENS) to customs of the destination port where goods enter the European Union (see Figure 2).

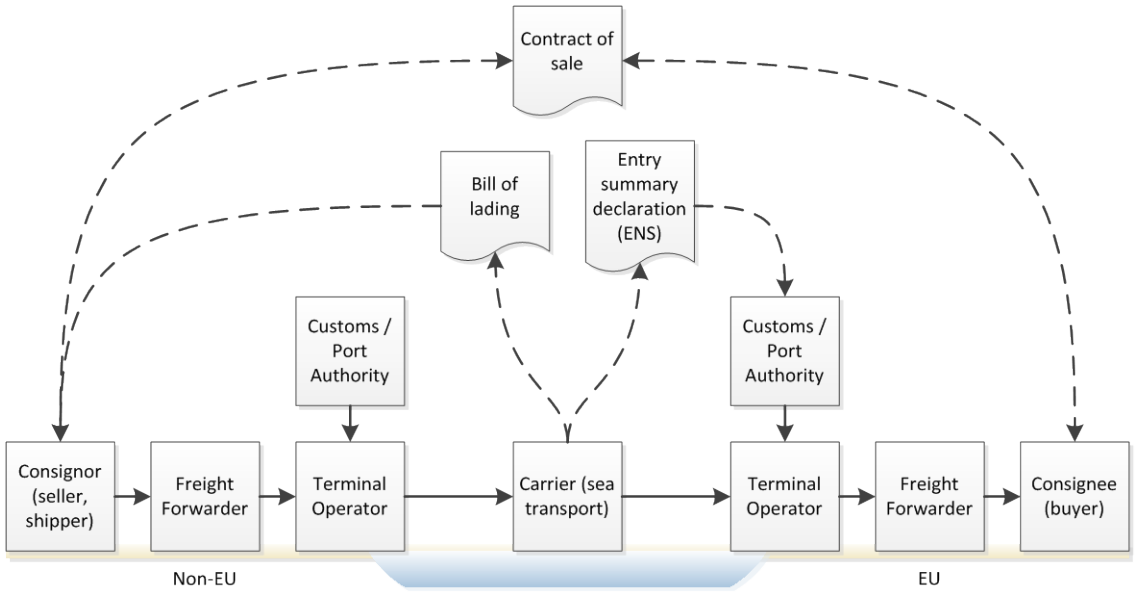

Figure 2: International flow of goods over sea with bills of lading / ENS issued by carriers adding pre-printed clauses to avoid legal responsibility in the current system

From a legal point of view the goods descriptions on the bill of lading and ENS can be used as proof of shipment. As such the ENS can be used for control purposes by customs. In addition the bill of lading can be used for commercial purposes in that it can prove that carriers can be held legally responsible for transportation of the goods on behalf of consignors.

To avoid legal responsibility, carriers often add pre-printed clauses to bills of lading / ENS such as “particulars furnished by shipper”, “quantity, quality, etc. unknown” or “said to contain” (carrier’s “dance” around the description, Hesketh, 2010, p8). This is understandable; carriers are often unable to verify which goods they have received from consignors due to e.g. sealed or locked containers and therefore avoid legal responsibility altogether. Overall the incentive for carriers to avoid legal responsibility is rather large since it poses financial advantages in terms of preventing claims for cargo loss or damage as well as relatively low insurance fees. For example, according to international agreements such as the Hague-Vishby Rules and Rotterdam Rules the maximum liability for carriers with respect to consignors in case of loss or damage of containerised goods is approximately $600 per container. If the carrier would be able to access information that the goods in the containers they are transporting are of higher value (e.g. via the Cassandra Pipeline) their liability in case of loss or damage would increase proportionally. Furthermore, avoiding responsibility ensures that carriers cannot be held accountable by customs when illegal goods are found in containers on their ships. Hence, a key issue that emerged from the Cassandra project revolves around the fear of carriers that the improved supply chain visibility due to the Cassandra Pipeline will increase their exposure to insurance and legal claims regarding the goods they are transporting on behalf of consignors, resulting in potential financial losses.

4.2 Issue 2: Sharing (Commercially Sensitive) Source Data

Many partners in the international supply chain are dependent on the quality of the data they receive. At present supply chain data provided by carriers to customs / port authorities often is of relatively low quality resulting in authorities frequently not knowing which goods are passing by. As mentioned before, a principal objective of the Cassandra Pipeline is to increase international supply chain data quality by obtaining data from the source enabling governments and businesses to conduct higher quality risk analyses. "The best party to provide quality information about the goods being transported is the original seller or another actor that 'packed the box'" (Klievink et al., 2012, p15). In other words, high quality source data for the Cassandra Pipeline should be made available by the consignor or the freight forwarder packing the box. For practical reasons freight forwarders are invited to share source data through the Cassandra Pipeline.

However, freight forwarders are not necessarily inclined to share source data through the Cassandra Pipeline for two reasons. First, the data can be commercially sensitive which could result in freight forwarders potentially being bypassed by partners further up the supply chain once these partners know who originally produced the goods (Klievink et al., 2012). This is supported by Cassandra project documentation in which freight forwarders indicated a moderate lack of trust between supply chain parties as a barrier to data and risk sharing (2012a). The sharing of commercially sensitive source data issue is illustrated by a Cassandra dashboard demonstrator for UK Customs based on source data from China provided by a freight forwarder. The issue expressed by UK Customs was that required source data was not made available to them via the dashboard. The freight forwarder understandably concealed required source data because this data was commercially sensitive and they feared that sharing could result in the data appearing in a Cassandra demo or in public Cassandra project documentation.

Second, commercially sensitive or not, the question remains whether freight forwarders will consistently share high quality source data through the pipeline since sharing is not necessarily beneficial for them. It seems likely that some freight forwarders will put in more effort than others, similar to the current situation in which carriers are providing supply chain data to EU customs (via ENS). Hence, a key adoption issue for designers of the Cassandra Pipeline is that freight forwarders are not necessarily inclined to share source data through the pipeline because 1) the data can be commercially sensitive which could result in being bypassed and 2) data sharing is not necessarily beneficial for them.

4.3 Summary

In short, the aforementioned data sharing issues regarding the Cassandra Pipeline revolve around difficulties for designers to persuade carriers and freight forwarders to adopt the pipeline information infrastructure concept. As such the issues illustrate the bootstrap problem of Hanseth and Lyytinen (2010) which refers to designer difficulties in gaining momentum for information infrastructures when the user community is still small.

5 Potential Data Sharing Solutions

This section first presents two solutions that emerged from the Cassandra project proposing how the aforementioned adoption issues regarding the Cassandra Pipeline can possibly be solved. Hereafter solutions proposed by the design theory for dynamic complexity in information infrastructures of Hanseth and Lyytinen (2010) are included.

5.1 Proposed Solution 1: Restricted Open Access

The Cassandra project clarified that data governance regarding who gets access to which data in the Cassandra Pipeline is required distinguishing between: open access, restricted open access and closed access. As explained in detail in Cassandra project documentation (2012b), the Cassandra Security Framework defines effective ways to securely enable data sharing between supply chain partners through the Cassandra Pipeline, recommending to protect shared data through application of encryption mechanisms, enabling identification and authentication methods as well as security protocols for protection against unauthorised access. Using communities and by distinguishing among data access levels, access to certain data in the Cassandra Pipeline for certain supply chain communities can be restricted, distinguishing for example between commercial data and transport data (Pruksasri et al., 2013). Interestingly, all supply chain data can be transferred through the Cassandra Pipeline using the current IT infrastructure of supply chain partners while certain specific data can still be hidden for certain partners using data encryption methods. For example supply chain data can be transferred through the Cassandra Pipeline using the available IT infrastructure of carriers while access to specific commercial data for carriers can be restricted.

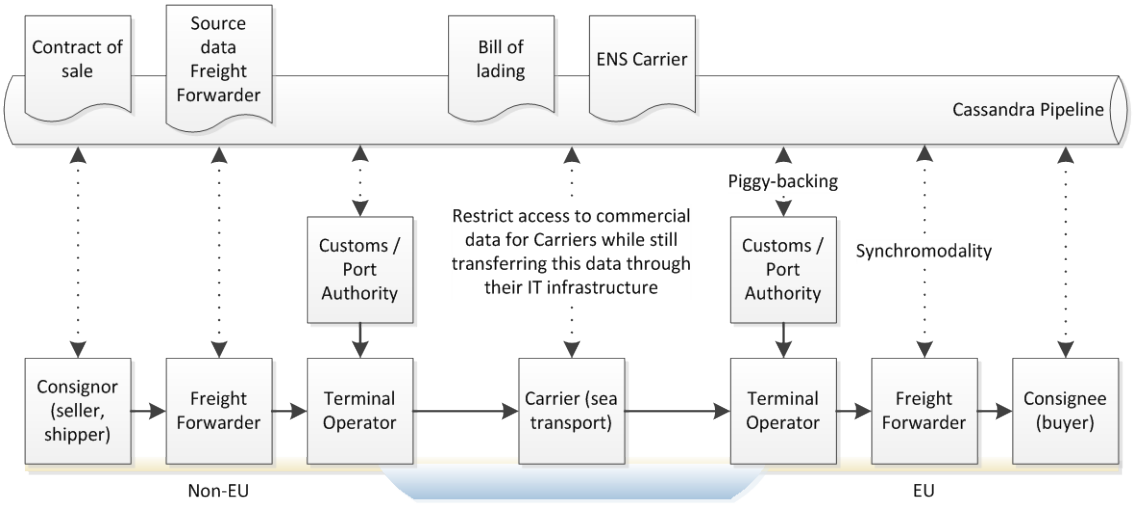

Figure 3: Restricting access to certain data for certain supply chain communities using the Cassandra Pipeline based on the Cassandra Security Framework

Restricting access to certain data for certain supply chain communities to the Cassandra Pipeline could solve several of the aforementioned adoption issues. First, restricting carriers' access to commercial data in the Cassandra Pipeline (e.g. consignor identity or goods descriptions) while still transferring this data through their systems using encryption methods could solve the issue revolving around carriers' increased legal responsibility in that they can continue to avoid liability when they cannot access the commercial data. Carriers are not exposed to increased claims of cargo loss or damage because they can legally demonstrate they do not know what is inside a container when

their access to commercial data in the Cassandra Pipeline is restricted. Second, the issue revolving around freight forwarders' reluctance to share commercially sensitive source data can be solved by restricting access to commercial data in the Cassandra Pipeline for carriers or other partners further up the supply chain. Freight forwarders do not longer have to fear they will be bypassed by carriers or other partners further up the supply chain in case access to their commercially sensitive source data is restricted for these partners, even if this encrypted data is transferred through their IT infrastructure.

It is key, however, to think carefully about the implications of restricting access to the Cassandra pipeline for certain supply chain partners. Restricting access seems to be in contradiction with the aforementioned central characteristics of information infrastructures being sharing, openness, heterogeneity, evolution, distinct IT capabilities and distributed and loosely-coupled control mechanisms (Hanseth and Lyytinen, 2010). Decreasing openness and sharing in the Cassandra Pipeline through a tightly-coupled centralised access control mechanism could reduce generativity, diminishing the potential benefits of the Cassandra Pipeline as an information infrastructure. However, completely open public access to the Cassandra Pipeline is not desirable as well, for example thinking about criminals accessing the pipeline to identify which containers on ships contain valuable goods.

The contradiction between open access and restricted access to the Cassandra Pipeline refers to the *paradox of control* of Tilson, Lyytinen and Sørensen (2010) explained by "opposing logics around centralized and distributed control [resulting in a] paradox of both more and less control" (p754). On the one hand generativity and trust in users is required for an information infrastructure to become successful, yet on the other hand practice often dictates some form of control is necessary as well to prevent potential abuse. Hence, designers of information infrastructures often need to achieve a balance of control between both extremes allowing for generativity on the one hand and preventing abuse on the other. "Apple's iTunes platform […] represents a "different" balance of controls, enabling on one hand a generative platform supporting millions of users and hundreds of thousands of applications, while on the other hand exercising strict control over application approval, payment terms, architectural rules, and many aspects of the internal operations of applications" (Tilson et al., 2010, p755).

For the Cassandra Pipeline the required balance of control suggests a form of restricted open access allowing trusted supply chain partners to access the pipeline if they wish for their own benefits while disallowing partners who will potentially abuse the information retrieved from the pipeline. Overall it is key for designers of the Cassandra Pipeline as an information infrastructure to think carefully about the implications of restricting access, maintaining a balance to allow for generativity while preventing potential abuse at the same time.

5.2 Proposed Solution 2: Non-obligatory Sharing

A complementary way to potentially solve the issue of freight forwarders' reluctance to share data through the Cassandra Pipeline is to make agreements regarding which data they will share. In essence there are two options for data sharing. On the one hand freight forwarders could be invited to decide for themselves which data to share (non-obligatory, bottom-up). On the other hand freight forwarders could be forced to share specific data with EU authorities through the pipeline (obligatory, top-down).

Again it is key for designers to think carefully about the implications of non-obligatory or obligatory data sharing through the Cassandra Pipeline, referring to the aforementioned paradox of control (Tilson et al., 2010). Sharing, (restricted) openness and distributed loosely-coupled control mechanisms seem necessary to allow for generativity and reap benefits from the Cassandra Pipeline as an information infrastructure. This is why non-obligatory sharing seems to fit best.

Combining both proposed solutions regarding data access and data sharing results in four scenarios as shown in Figure 4. The fifth restricted open and non-obligatory scenario seems to be most suitable to pursue for the Cassandra Pipeline, achieving a balance between allowing for generativity and preventing potential abuse.

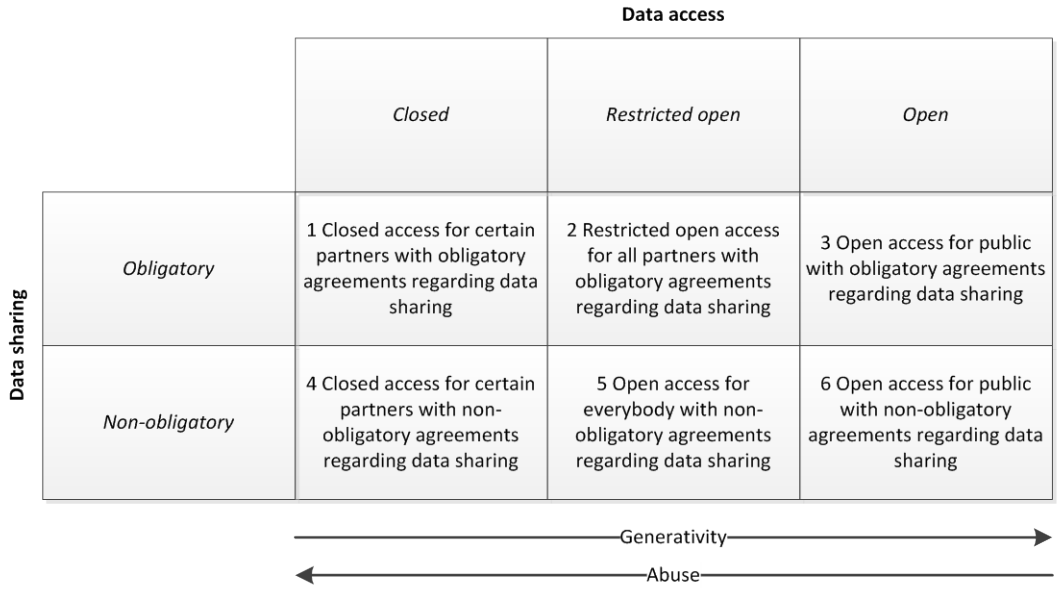

Figure 4: Data access and data sharing scenarios influencing adoption of the Cassandra Pipeline as an information infrastructure

5.3 Directions Proposed by the Design Theory for Dynamic Complexity in Information Infrastructures

Table 1 provides an overview of how three design rules of Hanseth and Lyytinen (2010) that relate to their "design initially for usefulness" principle could prove beneficial to tackle the aforementioned Cassandra Pipeline issues.

Design principle / design rule	Cassandra directions
1. Design initially for usefulness	
DR1. Target IT capability to a small group	Implement the pipeline for a small group of partners at start (e.g. freight forwarders and customs)
DR2. Make IT capability directly useful without an installed base	Focus on immediate and direct benefits for the small group of partners (e.g. freight forwarders and customs)
DR3. Make IT capability simple to use and implement	Obtain experience based on the use of simple prototypes and capabilities (e.g. prototype dashboards)

Table 1: Design rules proposed by the design theory for dynamic complexity in information infrastructures linked to the identified Cassandra Pipeline data sharing issues

The issue regarding carrier's increased legal responsibility can be tackled by implementing the pipeline for a small group of supply chain partners at start (DR1) without carriers who will possibly join later on. The issue regarding freight forwarder's reluctance to share commercially sensitive data can also be tackled by implementing the pipeline for a small group at start (DR1) leaving partners further up the supply chain that could bypass freight forwarders initially out of the loop.

The issue regarding freight forwarder's overall reluctance to share source data through the pipeline (commercially sensitive or not) can be tackled by creating immediate benefits for freight forwarders to start using the pipeline (DR2). As explained by Klievink et al. (2012), freight forwarders could for example benefit from their source data when they are able to use this data to decide which mode of transport to use when goods arrive in a port (e.g. rail, road or barge). This is called the synchro-modality concept. When freight forwarders can access source data via the Cassandra Pipeline they know which goods will arrive in a port and when. They can use this source data to choose suitable transport modes based on criteria such as timeliness, costs and CO2 emission. Bananas, for example, need to ripen and therefore can be shipped by slower yet cheaper and lower emission barge transportation whereas strawberries need to be transported by quicker yet more expensive and higher emission road transport. A simple prototype decision support system (DR3) that uses source data for synchro-modality purposes could convince non-EU freight forwarders to share source data through the pipeline for their EU counterparts.

6 Conclusions

The aforementioned data sharing issues regarding the Cassandra Pipeline that revolve around carrier's changing liability and freight forwarder's reluctance to share source data can be potentially solved through restricted open access and non-obligatory data sharing. In addition design rules of Hanseth and Lyytinen (2010) can be applied, clarifying that the recommended way for designers of the Cassandra Pipeline to gain momentum is by starting small, persuading supply chain partners to join using simple prototypes and gradually expand in correspondence with the partners.

It is key, however, that designers of the Cassandra Pipeline as an information infrastructure think carefully about the implications of restricting access and non-obligatory or obligatory data sharing. A balance of control is required both allowing for generativity and trust in the pipeline line while preventing potential abuse of the pipeline at the same time. Designers of information infrastructures need to achieve a careful balance between traditional top-down design approaches to prevent abuse and bottom-up experimental design approach to allow for generativity.

Future research will focus on further identification of issues in the international supply chain over sea and air that could prevent adoption of information infrastructures. The issues will be derived from new case study material and included in a framework. In addition, similar to Aanestad and Jensen (2011) for the healthcare domain, future design efforts will focus on creating and evaluating supply chain solutions based on the identified issues to complement the work of Hanseth and Lyytinen (2010) and formulate a comprehensive design theory for information infrastructures that will be validated through instantiated solutions.

References

Aanestad, M., & Jensen, T. B. (2011). Building Nation-wide Information Infrastructures in Healthcare through Modular Implementation Strategies. The Journal of Strategic Information Systems, 20(2), 161-176.

Avital, M., & Te'Eni, D. (2009). From Generative Fit to Generative Capacity: Exploring an Emerging Dimension of Information Systems Design and Task Performance. Information Systems Journal, 19(4), 345-367.

Benbya, H., & McKelvey, B. (2006). Toward a Complexity Theory of Information Systems Development. Information Technology and People, 19(1), 12-34.

Cassandra-project.eu. Retrieved 11-03-2014, from http://www.cassandra-project.eu

Cassandra. (2012a). Cassandra - D1.2 - User Requirement Report and Business Drivers.

Cassandra. (2012b). Cassandra - D3.31 - Data Security Framework.

Gregor, S., & Jones, D. (2007). The Anatomy of a Design Theory. Journal of the Association of Information Systems, 8(5), 312-335.

Hanseth, O., & Lyytinen, K. (2010). Design Theory for Dynamic Complexity in Information Infrastructures: the Case of Building Internet. Journal of Information Technology, 25(1), 1-19.

Hesketh, D. (2010). Weaknesses in the Supply Chain: Who Packed the Box? World Customs Journal, 4(2), 3-20.

Hevner, A. R., & Chatterjee, S. (2010). Design Research in Information Systems: Theory and Practice. New York Dordrecht Heidelberg London: Springer.

Holland, J. H. (2006). Studying Complex Adaptive Systems. Journal of Systems Science and Complexity, 19(1), 1-8.

Janssen, M., Chun, A. E., & Gil-Garcia, J. R. (2009). Building the Next Generation of Digital Government Infrastructures. Government Information Quarterly, 26, 233–237.

Klievink, A. J., Van Stijn, E., Hesketh, D., Aldewereld, H., Overbeek, S., Heijman, F., & Tan, Y. (2012). Enhancing Visibility in International Supply Chains: the Data Pipeline Concept. International Journal of Electronic Government Research, 8(4), 14-33.

March, S. T., & Smith, G. F. (1995). Design and Natural Science Research on Information Technology. Decision Support Systems, 15(4), 251-266.

Pruksasri, P., Van den Berg, J., Hofman, W., & Daskapan, S. (2013). Multi-Level Access Control in the Data Pipeline of the International Supply Chain System. In P. Chuan, V. Khachidze, K. W. L. Ivan, Y. Liu, S. Siddiqui & T. Wang (Eds.), Innovation in the High-Tech Economy (pp. 79-90). Berlin Heidelberg: Springer-Verlag.

Sol, H. G. (1982). Simulation in Information Systems Development. Groningen: Doctoral Dissertation, University of Groningen.

Tan, Y., Bjørn-Andersen, N., Klein, S., & Rukanova, B. (2011). Accelerating Global Supply Chains with IT-Innovation: ITAIDE Tools and Methods: Springer.

Tilson, D., Lyytinen, K., & Sørensen, C. (2010). Digital Infrastructures: the Missing IS Research Agenda. Information Systems Research, 21(4), 748-759.

Wikipedia.org. (2013). Cassandra. Retrieved 11-03-2014, from http://en.wikipedia.org/wiki/Cassandra, http://nl.wikipedia.org/wiki/Cassandra_(mythologie)

Winter, R. (2008). Design Science Research in Europe. European Journal of Information Systems, 17(5), 470-475.