A CONCEPTUAL FRAMEWORK FOR AN INTEROPERABLE ONLINE IDENTITY MANAGEMENT SYSTEM

by

Daniel Lee Sarmiento

A Thesis Submitted in
Partial Fulfillment of the
Requirements for the Degree of

Master of Science
in Business Administration

at

The University of Twente

28 February 2014

ABSTRACT

Backed by a variety of research in online trust, this paper presents a conceptual framework for a system which would help to secure online social networks and, in doing so, encourage participation in them. The focus of the research examines current identity models already in place and compares them to the general body of identity theory. All of the presiding information is examined within the context of what will be called the "dimensions of identity."

With these dimensions defined, developers of online identity can have a more optimistic expectation for an interoperable identity system that supports the social capabilities of the internet. The resulting conceptual framework provided here is meant to serve as a component of a larger effort – the identity ecosystem – in which multiple parties collaborate in ensuring the integrity of the internet and its users.

I. INTRODUCTION

As more and more aspects of our personal lives go online, there is a congruently increasing need to establish trusted identities on the internet in order to provide for more secure virtual interaction. Current attempts to do so have not only been marginal in their effectiveness, but have also been narrowly focused on ecommerce, or more simply, on online transactions involving monetary exchange. While the necessity of such internet identity systems is clear, existing services fail to address the exponential growth of online social networks. Much research has shown that the development of online socialization has been sustained by a generally uninhibited trust of the networks supporting it. But in recent times, this unfettered trust has been threatened as research and media reports have showcased instances of cyber-related crime such as stalking, sexual abuse, and violence (Wall, 2007).

Backed by a variety of identity research, it is the aim of this paper to present a conceptual framework for an interoperable system which would help to secure online social networks by harnessing the collective resources of online stakeholders. Central to this proposition is a U.S. government initiative called the National Strategy for Trusted Identities in Cyberspace (NSTIC)

which serves as a cross-sectorial call to action for the development of an "identity ecosystem" on the internet (Obama, 2011). It subsequently prescribes several conditions that should be met in order to establish such an ecosystem and further emphasizes that an effective system would likely be formed by multiple players operating with these conditions as a guideline. Systems should be: (1) privacy enhancing and voluntary, (2) secure and resilient, (3) interoperable, and (4) cost-effective and easy to use. It is acknowledged here that the NSTIC (Obama, 2011) is presented as a conceptual framework, as is the intent of this paper, however, the NSTIC also identifies a continuous evolution of thought in identity theory and the newer framework proposed here will be presented in the spirit of this evolution.

Sharing these ideals is the seminal research of Microsoft's Kim Cameron (2005) in his work, "The Laws of Identity"; a collaboration between industry leaders and academics, it has largely been accepted as a guideline for building a digital identity system (Hansen, 2008) and, like the NSTIC, alludes to the idea of establishing an identity ecosystem in which multiple identity systems should be utilized. Cameron (2005) further supports the development of a so-called "claims-based" identity system, where internet users can make evaluations about other users based on open participation within a network. While seemingly simplistic in nature, this idea is particularly important because of its focus on empowering the individual user in an identity system.

The research noted here, along with the growing body of online identity theory, is essential in the future development of trust on the internet. However, much of said research also falls into the previously mentioned genre of work which tends to neglect online social exchange as being at the forefront of cyber security. Consequently, the need for more well defined identities in social networks is accompanied by serious concerns for privacy and anonymity, and it is the incorporation of these concerns along with the guidelines set forth by existing identity research that will culminate in the findings of this paper in the form of a conceptual framework for an interoperable identity system which supports online socialization.

RESEARCH GOAL & QUESTION

Building on the foundation of existing conceptual frameworks for online identity and reputation management, it is the goal of this research to present the basis for a new, innovative system that will incorporate several techniques of its predecessors (which have largely operated in silos) and will also offer an interoperable system with the potential for adoption across the internet. Specifically, it will address the question: What factors are most important in designing an interoperable online identity management system that will enhance the trust of users while accommodating the rapid growth of social networks?

ACADEMIC AND PRACTICAL RELEVANCE

Because it is increasingly difficult to know with whom and to what we are connecting to on the internet, people are limited in what they can do online and are simultaneously exposed to growing dangers. While this holds true across online interactivity, the rapid expansion of social networking has posed many new challenges to securing online trust which have largely gone unaddressed. This paper offers a conceptual framework for a system that would help to establish more trusted identities in online social networks and, in doing so, address some of the current limitations of socializing on the internet.

STRUCTURE OF THE RESEARCH

The current lack of conformity in online identity terminology is a central problem in this thesis. Therefore, the definition of these disparate terms will be an essential first step in the research. Although achieving a universally accepted definition for these terms is unrealistic, the attempt to do so here will serve the larger goal of providing a context in which a collaborative approach to identity may be developed.

With a context in place, a theory of design will then be identified to guide the research. The structure provided by the design theory will be used to identify the crucial factors influencing identity development and guide the selection criteria for (1) a structured literature review and (2) a targeted industry analysis. The data retrieved from these studies will then be analyzed in order to establish key themes and, ultimately, the dimensions of identity. These dimensions will serve as the core of a proposed conceptual framework and of this study.

II. THEORETICAL FRAMEWORK

Context & Definitions

The concept of *identity* is one that has been the subject of much debate with regard to its role in society. Even a simple definition of the idea has evaded academics and social critics alike. Not surprisingly, recent attempts to define *digital* identity have similarly failed to reach a consensus and with constant technological innovation, identity research has continued to face new obstacles. This paper takes a new approach to defining digital identity by dividing it into several distinct dimensions. This approach will not only serve to distinguish the constituent parts of digital identity, but will serve as a basis for a conceptual framework for an interoperable online identity management system. These dimensions will also provide a context for understanding digital identity research and for future analysis. These dimensions must necessarily offer a distinction from any preconceived or generic definitions currently in existence. Prevailing definitions, however, will be crucial in providing a background for this research and, as such, will be drawn upon frequently.

What is Identity?

As a social construct, identity has had a complex history in scientific research. Disciplines ranging from sociology to anthropology to philosophy offer varying interpretations of identity, but, as suggested by Deaux (1993), an interdisciplinary concept of identity can help to inform

future research. Deaux (1993) offers a more universal notion of identity as "a way that we, as cultural observers, […] can describe certain aspects of individual definition and behavior" (p. 102).

Deaux (1993), who emphasizes that identity is both personal and social, also points to the importance of a context in which identity exists. This calls into question the differences in identity from a contextual and cultural standpoint. Drawing on the interplay between the two, Tajfel's (1978) seminal work suggests that identity emerges from the context of intergroup relations. Deaux (1993) goes as far as suggesting that this intergroup context is the result of contextual and cultural inputs of identity. More plainly, Deaux (1993) posits that "what is personal or social depends on the particular fit on an individual to context" (p. 103). Contexts – especially in the digital age – have been seen to constantly shift and to do so with such rapidity that individuals' identities have evolved in a similar fashion. Keeping in mind these mass contextual shifts, we must also consider the cultural (or ethnic) aspect of identity.

It has been suggested by some that within social anthropology, the notion of "identity" has largely been defined in terms of ethnicity – or "ethnic identity." It is further posed that the ethnic makeup of one's identity is directly related to his or her sense of solidarity within a community and a sense of "consciousness of sharing characteristics" (Sökefeld, 1999). However, this sense of solidarity and sameness, as Sökefeld (1999) points out, can have limiting effects in defining modern identity. He suggests that rather than "sameness," it is "difference" which offers contrast to defining identities and – more helpfully – emphasizes plurality. Simply put, identity can only exist if there is more than one identity (Sökefeld, 1999). This, it may be inferred, is particularly important with regard to identity on the internet and is a fundamental concern to this paper (i.e. how can individual users be differentiated in an anonymous and undifferentiated environment?). Sameness and also anonymity are intrinsic to online identity, which make the establishment of a unique and differentiated identity all the more challenging.

Given these challenges, we must not stray too far from the social concepts of identity in analyzing identity online. Sociality, or the tending to associate with social groups, is derived from anthropological practices to understand how individuals relate to one another (Bouman,

2007). These relations can inform, and are in fact central to, the definition of identity. It follows logically then, that sociality is a central concept in the design of online reputation systems.

Bouman (2007) holds that it is sociality rather than functionality that is the most important concept in social software systems. It is similarly posed here that this is particularly true for online reputation systems. The notion of building identities within an online social system is one that Bouman aligns – as is done here – with real world social groups.

What is Digital Identity?

In his research, Kim Cameron (2005) aims to define digital identity with regard to two of its fundamental components: subjects and claims; both of which require definition in their own right. Cameron (2005) defines a digital subject as a "person or thing represented or existing in the digital realm which is being described or dealt with" (p. 4). He defines a claim as an "assertion of the truth of something, typically one which is disputed or in doubt" (p. 4). So then, in simpler terms, digital identity is a set of claims made by one digital subject about itself or another digital subject.

Palfrey & Gasser (2007) of the Berkman Center for Internet and Society share some of Cameron's (2005) ideas on digital identity, but also note the limitations of a claims-based definition as simply a bundle of data, less tied to the individual than a personal identity. It is not, however, Palfrey & Gasser's (2007) dissention from Cameron's (2005) description of digital identity which is of particular interest to this thesis, but rather, their emphasis on the individual within a digital identity system.

On the internet, an individual identity can be established by joining both real world and digital characteristics such as passwords or biometrics. In this sense, attributes (such as name, age, height, employer, address) are connected to an individual. These attributes may be permanent or temporary, inherited, acquired, or assigned. Biometrics are determinate of biological and

behavioral characteristics (such as fingerprinting, voice recognition, and retina scanning) and can, in some cases, be used for consistent online authentication.

There are a multitude of dimensions that could compose a single digital identity, each of which with varying degrees of reliability and verifiability. Specifically in the context of online social interaction, attributes such as gender, age, and criminal background are of particular importance when choosing partners for socialization. This is generally the case for offline socialization as well, but there are two (not unrelated) assumptions, fundamental to the internet, which create new challenges to digital identity: that of privacy and of anonymity.

While many of the prevailing online social networks have flourished with little appropriations for privacy and anonymity (Hampton, Session Goulet, Rainie, & Purcell, 2011), with their burgeoning populations and increased concerns of public safety, these networks have been forced to deliberate the specifics of these concepts as being critical to online identity.

What is digital identity interoperability?

Creating a malleable identity system while effectively supporting security, privacy and anonymity on the internet is, by some accounts, one of the main motivations for the constant dialogue regarding digital identity interoperability (Palfrey & Gasser, 2007). This dialogue, however, remains in its infancy and consequently, no single definition of digital identity interoperability has emerged. This is in part because of the various types of digital identities; many of which have unique approaches to interoperability (a definition must be accommodating of this and therefore would be broad in nature).

For these reasons, and in the case of this research, the definition of digital identity interoperability mirrors that of Palfrey & Gasser (2007) as “a constantly shifting interconnection among ID users, ID providers, and ID consumers that permits the transmission of Digital ID information between them via a secure, privacy-protected channel” (p.11).

Palfrey & Gasser (2007) also suggests establishing a general group of stakeholders. These groups will be adopted to inform this research in further examining existing identity systems and are detailed as follows (p.11):

- Individuals (also referred to as users or subjects) – who want to be able to share aspects of their identity efficiently and securely regardless of the service or platform, with at least some level of ID portability;

- Relying parties (usually providers of services individuals want to use) – who want easy and secure access to accurate, timely, and relevant information about individuals from any source to maximize the value of their trust relationships and better serve their users, while limiting their own exposure to risks of a data breach;

- ID providers – who want effective and sustainable means to provide Digital ID services to any user and any relying party; and

- Society as a whole – which wants to balance convenient and secure authentication and accreditation with other social needs such as privacy.

Identity and Reputation

Identity and reputation are, in many ways, interrelated; this is especially true in an online context. In the traditional sense, both identity and reputation are defined as social concepts. However, their social implications were largely diminished when the internet was in its infancy; anonymity (for better or for worse) was the hallmark of the early internet. More recently, we have come nearly full circle as online socialization is now very much the norm and identity and reputation have, again, proven to have great social significance.

Presently, both online identity systems and reputation systems have been implemented and researched ubiquitously in the realm of cyber security. While each has been implemented in broad contexts, they have consistently been connected to one concept: trust. Whether it is to secure and facilitate ecommerce or to support online social networks, identity and reputation systems have always been designed to enhance trust (Ubois, 2003).

Because identity and reputation have remained social concepts in an online context, it is important to remain socially-minded in trying to define the terms (Mui, Motashemi, & Halberstadt, 2002). At the most basic level, the two remain relativistic to their environments, this is largely due to a high degree of subjectivity with regard to perception; identity being internally perceived and reputation being externally perceived. Still, even with the socially-constructed, perception-based definition of identity and reputation, contemporary systems and theories have begun to blur the line between the two. For example, in Cameron's Laws of Identity (2005), digital identity is posed within the framework of how we identify "who and what [we] are connecting to" – in other words, an external perception of identity. Meanwhile, Sulin Ba (2001), through her concept of transference-based trust (TBT), presents the idea of reputation as becoming part of an individual's identity, resulting in what can clearly be called an internally perceived concept.

As the defining characteristics between identity and reputation continue to converge, their goals online have, similarly, begun to align. As will be shown, this is especially true in online social networks. Facilitating online interaction and exchange trough identity and reputation management, once again, brings us to the notion of trust. Before addressing the role of trust in internet identity, we will first explore two concepts central to trust itself.

Privacy & Anonymity

Whittemore (2011) has attributed the innovative and transformational properties of the internet to what he called its "beautiful chaos." The internet, given its scale, has historically been a largely unregulated body and many experts, such as Whittemore, have maintained that

this is the single most important characteristic which has enabled the precipitous free-flow of information, and consequently of innovation, on the internet. Given this consensus, many of the attempts to regulate the internet have been met with contempt from individuals and resistance from web-based businesses. Regardless of the varied motivations for these objections, many of them can be reduced to the basic right to privacy and the desire for anonymity.

It is no surprise that, when it comes to online identity, the concepts of privacy and anonymity have been important, if not central, ideas. And while they are frequently discussed collectively, privacy and anonymity each raise unique and relevant concerns. The paradox of online privacy is one that has very clear generational lines – with older users and younger users on opposite ends of the spectrum of privacy concerns (Hampton et al., 2011). But the spectrum itself has been in a constant shift in the form of a steadily increasing laxity with regard to the privacy of online interaction. Generally speaking, online users have obliged in surrendering personal information in order to access more services. Not unexpectedly, this has led to decreased anonymity in many social settings and an ever-more pronounced online "footprint" for users. Many suggest that this footprint is the precursor to, if not the foundation of, a unified and recognizable online identity (Madden & Smith, 2010). The seeming inevitability of online identity not only underscores the necessity of identity research and development, but also calls into question the ethical and social composition of Web 2.0 and its successors. Such questions will, for purposes of scope, not be addressed specifically hereafter, but rather will serve as a litmus test with the intent of informing the proposed framework.

Identity and its relationship to Trust and Reputation

As defined by Duan & Liu (2012), trust is a subjective probability by which an individual expects that another individual will perform a given action on which his/her welfare depends (p.326). Reputation refers to the public opinions regarding trust on a certain object. With what appears to be a fundamental link between trust and reputation, what connection do these two concepts have in relation to identity? For answers, we can again turn to the theory of Bouman et al.

(2007) on sociality and the self. Noting identity as implicative of the construction of the self, Bouman et al. (2007) link all theories of identity with the social formation of the person and complex relations between individuals and groups.

The distinct definitions offered by Duan & Liu (2012) and Bouman et al. (2007) seem to be quite naturally linked, but each stop short of stating the link explicitly. Here, it is proposed that that link is sociality itself. Sociality (or social formation), playing a central role in many theories of identity, can be broken down into many constituent parts and – with Duan's (2012) definition of trust and reputation – we can now deduce more clearly why the concepts must be addressed jointly when discussing identity management. All of the concepts discussed being inherently social concepts – and which have significant influence on one another – to address them in isolation becomes more and more damaging to any comparative identity theory.

This lack of conformity in identity theory is symptomatic of the challenges which face it today. There are risks not only in examining the concepts of identity theory in isolation, but also in the practice of identity management. With competing forces in the development of online identity, many disparate identity providers have emerged, however, the result of this inundation is a problem which finds itself at the center of identity management: identity in silos.

Identity in Silos

The internet has been widely criticized for its intrinsic and fundamental lack of security and privacy, a critique that, in many cases, has been accompanied by the consolation that it has been this absence of regulation which has allowed the internet to thrive as a medium of exchange. However as new mediums have evolved, so too have the social implications of identification (or lack thereof) on the internet. As a result, but more commonly as a matter of business, many independent identity and reputation management systems have emerged and have been briefly discussed in this research. Whether in the form of a feedback system supporting ecommerce (as in eBay or Amazon) or as an independent identification provider

offered as a security solution (OpenID or DandyID), an innumerable and irreconcilable mass of online identities has done little to enhance trust on the internet.

Online trust, therefore, has become both a highly coveted commodity in business and also a chief concern of government and the public interest. Online social networks have developed ways of rating and identifying their members and enterprising governments have gone as far as issuing nationalized IDs for its citizens (Lim & Sanchez, 2009). But even on the broad scale of identification at the national level, the problem of interoperability persists. Identity providers operating in silos have, of yet, been unable to address the vastness of global social exchange which has come to embody the internet today.

What types of online identification currently exist?

Although the environment for online identification is constantly in flux and is in a largely developmental state, several prevailing approaches to identity can be identified. Jensen, Davis & Farnham (2002) identify three main categories for online identification: ranking systems, rating systems and collaborative filtering systems. Ranking systems use quantifiable measures of users' behavior (implicit information) to generate a profile, and are hereafter referred to as "Profiling" systems. Rating systems use explicit evaluations given by users and are hereafter referred to as "Reputation Ratings." Collaborative filtering systems weigh explicit or implicit evaluations by based on past interactions between users and are hereafter referred to as "Linkage" systems.

Through their research on Decision Support Systems, Basu & Muylle (2003) identify two further forms of online identification: authentication and certification. In combination with the research of Jensen et al. (2002) the following five approaches to identity will be examined:

- Profiling – using an algorithm (of selected inputs) to create a user profile.
- Reputation Ratings – describes how credible a user is based on past experiences with other users.

- Linkage - describes connections between people (i.e. linkage to Google credentials)
- Authentication – verification of the data or credentials provided during a user's attempt to gain authorization to do something online.
- Certification – issuing of a unique endorsement (or certificate) such as a digital ID number.

The Identity Ecosystem

With the varying approaches to identity, it is easy to see how a single united online identity would prove to be evasive. While the use of these approaches has almost completely come to fruition independent of each other, some current efforts have surfaced to propose collaboration in online identification.

Obama (2011) defines the identity ecosystem as "an online environment where individuals and organizations can trust each other because they follow agreed-upon standards and processes to identify and authenticate their digital identities" (p. 2). Although a seemingly utopian prospect, the idea of an identity ecosystem serves its purpose in providing a vision for a unified front in addressing the challenges of online identity. And while a set of "agreed-upon standards" may not be feasible in the inherently disordered context of the internet, the establishment and broad-based adoption of a shared value system – as many experts have attested (Backhouse, 2006) – would certainly do well to enhance trust on the Web. The identity ecosystem, for all intents and purposes, represents the combined effort of a wide array of actors in establishing trusted identities on the internet and, by bolstering the credibility of individual users, can support the expansion of online social networks.

III. Methodology

RESEARCH DESIGN THEORY

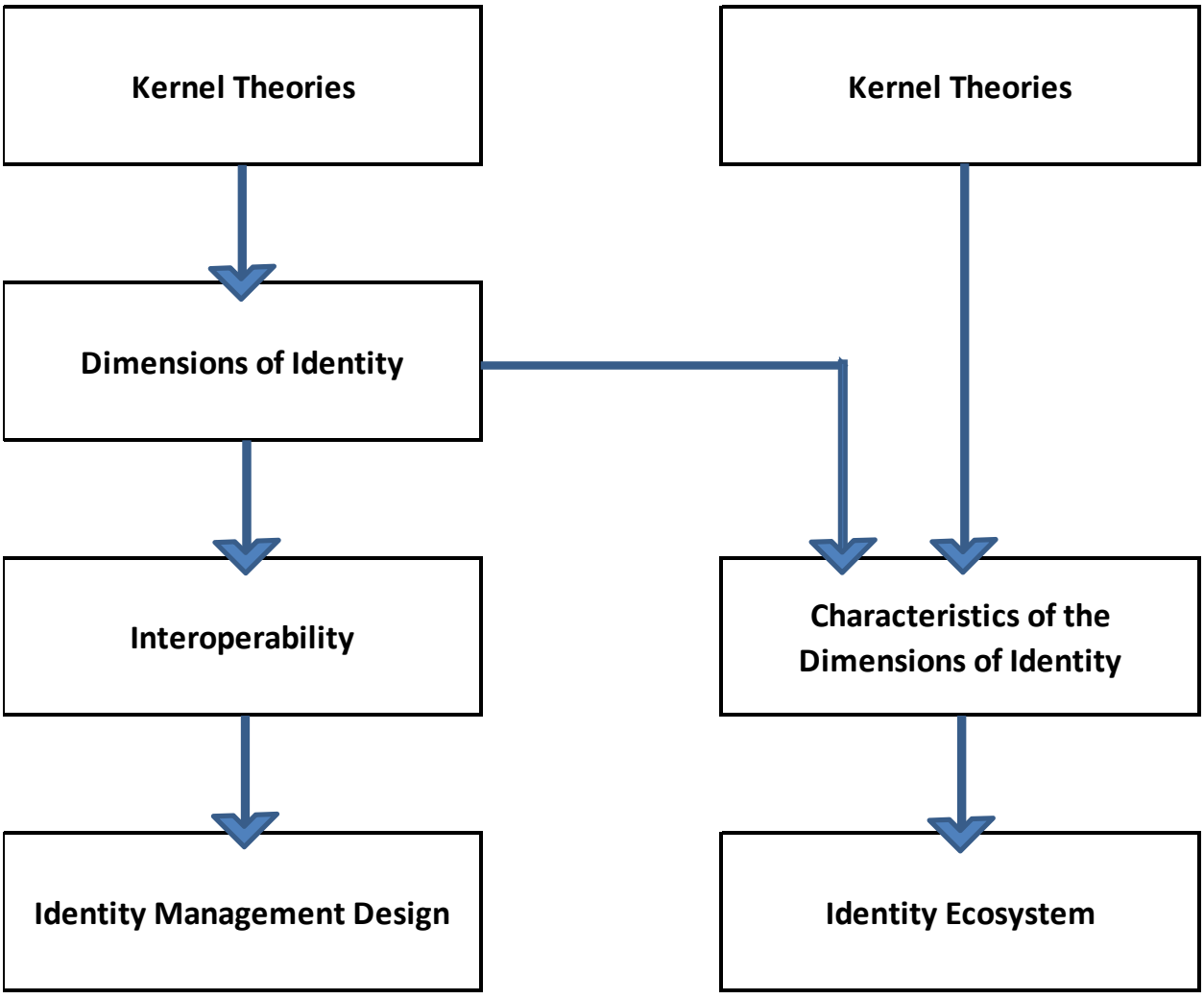
Keeping in mind the contemporary theoretical landscape of technology and the development of information systems, a conceptual framework could more simply be viewed as a "business model." And rather than explicating the differences between the two concepts, Osterwalder, Pigneur & Tucci (2005) present a unified notion of a business model being best understood as a "conceptual view of a particular aspect of [an organization]." And finally, using a conceptualization to capture business models facilitates their graphical presentation (Gordijn & Akkermans, 2001). The steps taken in this research will aim to illustrate a graphical depiction of a foundation for interoperable identity management.

From a theoretical standpoint of reputation management, several parallels can be drawn from a slightly more specialized field as presented by Walls, Weidmeyer & El Sawy (1992) in their theory of vigilant executive information systems (EIS). Just as in reputation management, Walls et al. (1992) cite the insufficient amount of theoretical development which directly informs the conceptual characterization of EIS and which should guide its design. Walls et al. (1992) use the figure and table in Appendix C to delineate these theoretical foundations and outline in detail how design theory can help to develop information systems. This comprehensive approach will serve to offer a broad landscape for future development.

The exact figure used by Walls et al. (1992), however, will not translate directly for use in the development of an interoperable identity system. So, as is shown is Figure 1, the model has been modified to demonstrate the design theory involved in this research. The components of this design theory will be informed by a systematic literature review and a targeted industry analysis. More specifically, the kernel theories mentioned will be gleaned from the cross-section of the literature in identity theory. These kernel theories will lead to the establishment of a concept central to this research: the dimensions of identity. These dimensions will then be extrapolated to show (1) how they influence interoperability and how this influence can lead

product design, and (2) how the characteristics of the dimensions themselves will contribute to the identity ecosystem as a whole.

Figure 1. Revised Design Theory Structure



As identified in Figure 1, kernel theories serve to govern the requirements of design theory, and given their importance, should be taken from a variety of credible and vetted sources. And with the urgency of online trust mounting, it is no surprise that a wealth of knowledge has

emerged with various intended solutions. Because the issue of trust, and more specifically online identity, is not an issue isolated to a specific industry, the research informing this paper will be equally as diverse.

The NSTIC charts a course for the public and private sectors to collaborate in raising the level of trust associated with the identities of individuals, organizations, networks, services, and devices involved in online transactions (Obama, 2011). This strategy will also help to inform my research in a number of ways. First, the aforementioned conditions for creating an "identity ecosystem" will be used to guide the development of the conceptual framework presented. Second, the NSTIC not only reinforces the social need for increased trust on the internet, but also attempts to delineate the roles of parties that should be responsible for the innovation of it. Third, it provides a clear context, in which identity systems can be developed.

Cameron (2005) takes a more broadly based approach and cites the fundamental flaws of the internet as being built without any way of identifying people and things with which we connect. In his research (notably sponsored by Microsoft) Kim Cameron lays out the seven essential laws that explain the successes and failures of digital identity systems: (1) User Control and Consent – technical identity systems must only reveal information identifying a user with the user's consent, (2) Minimal Disclosure for a Constrained Use – the solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution, (3) Justifiable Parties – digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship, (4) Directed Identity – a universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles, (5) Pluralism of Operators and Technologies – a universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers, (6) Human Integration – the universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks, and (7)

Consistent Experience Across Contexts – the unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies (Cameron, 2005, pp. 6-11). Like the NSTIC, Cameron's (2005) research has clear and apparent intentions in providing a foundational context in which identity management can be developed, but is similarly cognizant of the need for a multi-faceted approach.

The ideas in the research mentioned, along with a range of theories in the sphere of digital identity, have, whether directly or indirectly, influenced many incarnations of identity which have been put into practice in an online context. Existing systems have experienced varied degrees of success (of which is clearly subjective), but more importantly, none have offered a completely interoperable approach to identity. Nonetheless, two seminal texts - the NSTIC and the Laws of Identity - do portray foundational theories of interoperable identity and their requirements can be embodied in four key questions posed to identity system developers: (1) What type of data is needed? (2) In what context should a system be used? (3) What technological and human knowledge is needed? (4) What approach (methodology) to identity should be in place?

These questions embody what will hereafter be referred to as the dimensions of identity:

1. Data Dimension – What data is needed?
2. Use Dimension – In what context is the system ideally used?
3. Infrastructure Dimension – What technological and human means/knowledge is needed?
4. Methodology Dimension – What approach to identity is in place?
    a. Certification – issuing of a unique endorsement (or certificate) such as a digital ID number.
    b. Authentication – verification of the data or credentials provided during a user's attempt to gain authorization to do something online.
    c. Profiling – using an algorithm (of selected inputs) to create a user profile.

d. Reputation Ratings – describes how credible a user is based on past experiences with other users.
e. Linkage - describes connections between people (i.e. linkage to Google credentials)

SELECTION AND SAMPLE

Systematic Literature Review - A search in the PiCarta, Scopus, Google Scholar, and Web of Science databases was performed with a date range from January of 2000 through December 2012. Some articles were also identified using a manual search from bibliographies of relevant works. Some online articles and book chapters were also included. Papers containing the terms "online identity," "internet identity," "interoperable identity" and "online reputation management" in their title or abstract were identified. The abstracts of these studies (n =1285) were then reviewed to identity whether they contained information regarding the development of online identity.

Articles were included if they contained discussion on both online identity and any ideas pertaining to the development of it. Articles were also included if they discussed any joint efforts (interoperability) in instituting online identity or reputation management. Articles were excluded if discussion was limited to ecommerce with little or no mention of the social implications of online identity.

Lastly, I reviewed 422 studies which contained pertinent information regarding the dimensions of identity and 71 papers were identified. These papers were evaluated thoroughly and, after excluding duplicative material, the most relevant studies were included in the literature review and are cited in the reference list in Appendix A. The prevailing themes from the studies are detailed in Table 1 below.

Targeted Industry Analysis – This analysis will serve as a representative cross-section and comparison of some of the main contributors to the existing online identity environment. Many of the current systems have (or so they have claimed) added to the identity ecosystem by

augmenting their user base and helping to secure online identities through one of the types of online identification (certification, authentication, profiling, reputation ratings, and linkage.) Analyses and backgrounds of each of the systems will culminate in the creation of an Identity Management Table which will juxtapose the crucial characteristics of each system in order to identify their strengths and weaknesses as well as move toward a logical "next step" in online identity management.

DATA COLLECTION

The research tools described will provide a basis for comparison and extrapolation from which a conceptual framework for building trust in online social networks will be presented. The academic research used in this paper will be collected from university databases. Government and business resources for this paper will be collected from official websites (much of the research used from these sectors was created in collaboration with an academic institution.) It is important and appropriate to consult both private and public sectors, as they have proven to be highly influential stakeholders in the development of the internet and on people's interaction with it: business and academia as fore-thinkers and innovators and government as regulator.

DATA ANALYSIS

Both the systematic literature review and the targeted industry analysis will be represented in the format of a table in order to juxtapose data which would otherwise be difficult to compare. Of particular utility, is the table's comparison of competing theories and systems which had previously been unrelated and/or had been analyzed individually. In examining the systems and literature we can extract the most important contributors and detractors in identity management.

IV. RESULTS

In order for a more lucid comparison of the current online identity landscape, the following reputation management table was created to distinguish the defining characteristics of some of the market's prevailing identity systems. It should be noted that the table is not meant to be an exhaustive representation of the systems, but rather, a snapshot of each system and its characteristics most relevant to this study.

Table 1. Reputation Management Table

Identity/Reputation Management System	Data Dimension	Use Dimension	Infrastructure Dimension	Methodology Dimension
OpenID	Creation of a user profile using personal information	Eliminates the need for services to provide their own ad hoc systems and allows users to consolidate their digital identities	Network of Relying parties (RPs), exchange of an Identifier (OpenID), enabled by a User-agent program	Authentication
VeriSign Identity Protection Services (VIPS)	VIP Credential, Security Code	Added security for accessing sensitive information online	Network of RPs, physical credentials, User-agent program	Authentication, Certification
DandyID	Creation of a user profile using personal information	Single users possessing multiple site log-ins	Network of RPs, exchange of an Identifier (DandyID)	Linkage
eBay *(cont. on next page)*	Creation of a user profile using	Allows positive, negative and	Feedback repository, rating	Reputation Ratings

	personal information	neutral comments on a per-transaction basis.	system, rating parties	
Couchsurfing.org	Creation of a user profile using personal information	Allows positive, negative and neutral comments based on users' in-person interactions.	Feedback repository, rating system, rating parties	Reputation Ratings
Cisco Identity Services Engine (CISE)	Real-time contextual information from networks, users, and devices	Enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations.	An existing Cisco policy platform	Profiling
MyID.is	MyID.is Certified account (personal information certified by MyID.is staff)	Certify users' digital identity, and certify any content that they publish over the Internet	Digital Identity certification platform.	Certification
Windows Live ID (WLID)	An encrypted time-limited cookie stored on users' computer and a Triple Data Encryption Algorithm (TDEA) ID-tag	Single users possessing multiple site log-ins	Windows Live ID authentication server. Network of RPs, exchange of an Identifier	Authentication

Web of Trust	Four components to rate reputation - trustworthiness, vendor reliability, privacy, child safety	Allows Internet users to assess the trustworthiness of websites.	Community-based browser add-on	Reputation Ratings

*See Appendix B for a complete list of these websites

Where have current systems failed?

One notable failure in the reputation management table (and paradoxically the most commercially successful) is the eBay feedback system. Although it is firmly established as an economic (rather than social) giant on the internet, its online presence alone warrants consideration in the realm of reputation management. The eBay marketplace has facilitated countless transactions but has failed to address many of the social problems related with buyer-seller interactions online (Brown and Morgan, 2006). Specifically, eBay has been plagued by three core problems: ballot-stuffing, Pollyanna assessments, and creating a market for feedback.

Reputation systems like eBay are susceptible to ballot-stuffing which occurs when a seller can conspire with one or more buyers to engage in false transactions in order to bolster reputation (Bhattacharjee & Goel, 2005). This phenomenon is particularly prevalent where economic interests are at stake, but is certainly not unique to the sphere of ecommerce. Any online environment in which, for one reason or another, deviant actors set out to deceive other users is significantly at risk of decreased trust.

Resnick & Zeckhauser (2001) expose one of the main weaknesses of relying on feedback which is mainly provided voluntarily; namely, that it creates strong incentives to free ride, and quite possibly to Pollyanna (disproportionately positive) feedback. Outside of the obvious and (possibly unwarranted) advantages that eBay enjoys from having a misleadingly reputable usership, another related, but possibly more poignant flaw in their system is the negligible differentiation in the reputation of its users. This is, in effect, the essence of a reputation

system and eBay's failure to implement a measurable scale absent of bias has been heavily criticized in academic and economic research (Resnick, 2004).

In discussing eBay's attempt to address many of the shortcomings of their feedback system (mostly those of trust) Brown & Morgan (2006) are critical of what she calls a "manufactured reputation." They identify this contrived reputation as a direct result of the creation of a secondary market for eBay feedback. This secondary market puts a price tag on user feedback itself as sellers engage in, more or less, insignificant transactions, with the ulterior motive being the exchange (and ostensibly the sale) of feedback. Brown & Morgan (2006) emphasize how such a secondary market completely undermines eBay's attempts to secure trust in its system and stresses that emerging online networks and marketplaces should take the proper steps to avoid such an unneeded extremity.

It should be noted that failures of the eBay system are by no means unique to eBay, and in fact, are quite universal in online marketplaces (Bhattacharjee & Goel, 2005). What is particularly useful in characterizing the eBay system is to examine challenges commonly encountered when online reputation is tied directly to economic interest. Online social networks generally have, with some exceptions, more flexibility to establish reputation where the exchange of money is less prevalent. This is not to say that establishing credible reputations has been any more successful among social networks; in fact, it has led to the development of several third party reputation providers, some of which are presented in Table 1 above.

While companies like eBay and Microsoft have had very public failures in reputation management, many more attempts outside of the mass market have fallen short in creating a reputable interoperable online identity. The reputation management systems identified in Table 1 have been implemented with varying goals for online identity in mind, but none have been wholly successful in achieving universality, or more specifically, overcome the restrictions of identity in silos.

Where have current systems succeeded?

Some lesser known entities in Table 1 have, despite their comparative size, have established themselves at the forefront of reputation system innovation (Blitstein, 2009). Just as the internet has been swept by the wave of social networking, companies like DandyID and Couchsurfing.org have built systems to adapt with the times. These, and similar systems, have focused on the social implications for reputation and have attempted to harness the "power of the crowd." Many of the pioneering reputation systems have been developed independently of the traditional online marketplaces (e.g. eBay) and have begun to break down the barriers of siloed reputation by sharing reputation information. Because many of these systems remain in their infancy, it is difficult to measure their success, however, as the internet evolves and becomes more socially inclined, so too will a more socially-minded, trust-based reputation system come into necessity.

In one example, DandyId has attempted to consolidate internet users' ever-expanding number of online profiles by linking them to each other and creating one centralized identity or a "DandyID." This is an example of the emerging forms of reputation systems which utilize linkage as a means for establishing identity. Linkage, as it has been defined, requires multiple online profiles and aggregates the level of trust associated with each of them in order to present one united identity. Although not the first to combine multiple identities, DandyID has been innovative in the field by leading the shift to a "socially focused" identity – that is, one which harnesses the power of social networking. Traditional attempts (e.g. Microsoft Passport) at merging online identities focused on the reputation of the aggregate identity itself, whereas newer systems are utilizing the strength of the existing identities (e.g. Facebook and Couchsurfing profiles) in order to establish a system of transference-based trust. In essence, the reputation and trust built intrinsically into each of the emerging social networks is centralized into one trusted identity.

A similar approach has been taken by the aforementioned cultural exchange website, Couchsurfing.org. Their social network institutes a system of mutual trust ratings as well as physical address verification, but with its steady growth, it has continuously had to augment its

reputation system. Their business model is almost purely dependent on trust among its members and, in recognition of this, the site has partnered with Facebook in order to expand its trust base to what has become the largest social network online. While this has added another layer to their reputation system, Facebook has a trust deficiency in its own right and linking the two together by no means creates a perfect reputation system. Still, the power which can be found in the collaboration of networks and groups is one that has been underscored by many experts as a staple of future reputation systems (Tapscott and Williams, 2006).

How do these successes and failures relate to the dimensions of identity?

Even in examining a small cross section of reputation systems (as in Table 1), it can been seen that the approaches to reputation and identity are varied in terms of the dimensions of identity: data, use, infrastructure, and methodology. While the characteristics of the systems mentioned may be highly capricious, some patterns and similarities can be drawn.

The data dimension of identity, as represented in Table 1, can be implemented in a number of different ways. In both the eBay system and systems like that of DandyID, an independent and unique user profile is required in order to provide for a subjective rating system. Therefore, the data dimension, where user input is required, cannot necessarily be linked to reputation system failures or successes. However, the seemingly endless creation of user IDs and passwords is not only a nuisance but a significant security risk, and is therefore, a challenge to online identity.

The use-dimension of identity has in many ways been positioned as a solution to the problems created by the data dimension of identity. The use dimension, or scope, of several of the prevailing reputation systems has been aimed at consolidating or limiting the number of user IDs per person (e.g. WLID or DandyID). There are also systems, such as Web of Trust, which aim to empower the individual user by giving him or her the ability to make a determination of the trustworthiness of a host network. Conversely, systems like CISE aim to empower the network

itself by providing methods for enforcement. Whichever the case may be, the theme of trust empowerment has sprung up across online reputation and trust systems.

Within the sample examined in Table 1, the infrastructure dimension of identity generally points to two different approaches for the foundation of a reputation system: internal and external. Internal systems, such as those of eBay and Couchsurfing.org, rely on the feedback of their users to rate the trustworthiness of other users. External systems, such as CISE, MyID.is, and Web of Trust, utilize alternate platforms or "ad-ons" through which a user can be "transferred" trust via the perceived trust of his or her host network. There is no clear cut consensus on which of the two has had more market success, or even if the two cannot work in conjunction. What is apparent, however, are the structural differences in systems which do and do not have to support a system of ecommerce. In the past, these had been the majority of systems in which trust was an issue. But as we have seen, with the rise of social networks, online interaction is no longer just about buying and selling. The eBay and Couchsurfing.org infrastructures are similar in there composition, but with the removal of monetary exchange, the latter is able to utilize a much richer and more accurate reputation system – it is free of many of the issues previously addressed which are fundamental to the eBay system. All this being said, it is clear that neither online shopping nor online socializing are passing trends. Both need to be addressed when creating an online identity system.

The final dimension to identity, the methodology dimension, is characterized by five different approaches: certification, authentication, profiling, reputation ratings, and linkage. Certification, as in the case of MyID.is, requires a significant amount of infrastructural resources and has several relying parties. Given its resources-intensive makeup, it can be argued that such a system is also the most secure. While this may be true, one significant consideration for which this approach falls short is scalability. Of particular focus in this study is the application of reputation systems to the rapid growth of social networks; growth which can be exponential and, therefore, problematic in a resource-intensive system.

Another approach with somewhat rigid characteristics is authentication. Systems such as WLID and VIPS share some of the attributes of a certification-based system, but also differ in that

they focus on authenticating the individual user. Although this departure seems more feasible (making the individual part of the network more trusted in order to have the network itself be more trusted) it also exacerbates the problems of scalability. Just as with the certification approach, the authentication approach requires significant resources for proper implementation.

Reputation ratings systems have come to be a scapegoat, of sorts, for the criticism of online identity today (Bhattacharjee & Goel, 2005). While their shortcomings are evident, systems such as eBay's are still recognized as the pioneers in online reputation. Although this system is far from flawless, it is undeniable that it is a step forward from nonexistent alternatives. A reputation ratings approach, just as in an authentication approach, places emphasis on the individual. But unlike an authentication system, reputation systems have moved toward empowering the individual user – a shift that has, by no means solved the problems of online identity, but one which can be drawn upon for the future of it.

A profiling method also relates to the other approaches in that it too is resource-intensive. Systems such as CISE require an existing platform for networks to utilize its capabilities. One of the unique strengths that can be gleaned from a profiling system, however, is the creation of a resilient identity which takes into account multiple inputs and the presentation of a palpable identity which is perceivable to users both inside and out of the network. Profiling takes a third-party approach to identity by relying on "trusted" information and personifying it through its version on online identity (i.e. a profile).

As a natural progression, linkage is the newest approach to identity. Specifically because it aims to describe the connections between people (and connections between existing online networks), it has only been able to develop as more substantial (with regard to membership) online networks have been established. The particular strong point of the linkage approach is its scalability. A linkage approach aggregates existing reputation systems, whereby it strengthens its own reputation with the addition of each additional network. Granted, the argument could be made that a linkage approach only inherits the shortcomings of the alternate systems it combines; however as the most inclusive approach it would be most adept

in utilizing mass collaboration, and as defined by Tapscott & Williams (2006), the phenomenon of mass collaboration is the only way to harness the endless growth of the internet.

The dimensions of identity each, in some way, represent the future of online reputation and identity management. As is attempted in this research, it is important to analyze the varying approaches to identity and to single out those aspects which are most likely to be successful in keeping up with the growth of the internet. Because there is no "silver bullet" solution to the problems of identity, each of the dimensions of identity described above is acknowledged as offering significant contributions in moving toward a solution.

Current Studies in Identity Management

Below is a summary of the studies examined. In their review, several important themes arose which aligned with the focus of this research. These themes were (1) Collaboration: how relying parties can actively work together in the management of identity. (2) Interoperability: how ID providers can harness collaboration to create a dynamic and trusted online identity, and (3) Online Socialization: how society as a whole will be affected by changes in online identity.

These common themes were identified throughout each of the studies and their implications have been identified in the table below. The table is followed by further discussion on these implications.

Table 2. Literature Review

Date/Author	Implications for collaboration	Implications for interoperability	Implications for online socialization
Friedman , 2000	Dues-paying equilibrium	Resilient pseudonyms	Value-sensitive design
Ba, 2001	Community responsibility system	Intra-community contract enforcement	Transference-based trust building between communities
Cameron, 2005	Laws of Identity	Unified identity metasystem	Provide more certainty about who users are relating to in cyberspace
Jordan, 2003	Augmented Social Network	Persistent online identity	Facilitate introductions between people who share affinities
Madden, 2007	Managing or tracing a digital footprint	Persistent presence online	Increased searchability
Obama, 2011	Development of an identity ecosystem	Enable individuals to easily switch providers and harness market incentives to meet individuals' expectations	Charts a course for the public and private sectors to collaborate to raise the level of trust associated with online identities

Paci, 2009	Multifactor identity verification	Relying party and client exchange and verification	Unique descriptions of individual's and their relationships to others
Palfrey, 2007	Uniting of industry leaders	New markets created as a result of digital Id interoperability: competition for Digital ID itself and services built on top of a pervasive ID layer	Digital ID infrastructure could include greater privacy control

A Community Responsibility System

According to Ba (2001), community responsibility systems are social structures supported by technology. They are meant to facilitate trust building in online environments where interaction (both personal and impersonal) take place. Under the system which Ba (2001) proposes, the most important aspect, as it pertains to interoperability, is what she calls "intra-community" contract enforcement. As the term implies, Ba's (2001) system is based on the idea that multiple online communities should have a unified system (or metasystem) in which all members can be held accountable for their actions regardless of their community affiliation. While Ba's (2001) system is geared toward online market exchange, her idea has proven to be one of the earliest of its kind which had implications for reputation management in a social setting. In an interview, approximately eleven years after her paper was published, Ba disclosed (D. Sarmiento, personal communication, February 22, 2012) that her proposed system had failed to make any headway in the industry and that the project was all but abandoned in

the years that followed its presentation. In spite of this, its contributions to reputation theory may still be applicable today. Such can be said in the case of TBT which is a fundamental part of, not only intra-community contract enforcement, but also of many contemporary models for reputation and identity in social networks. The concept of TBT demonstrates how the market can collectively utilize the inherent trust of isolated communities so as to bolster trust of a larger community and facilitate greater online interaction. Particularly of note is its ability, or rather adaptability, in keeping up with an ever-growing online social landscape.

Multi-factor Verification

Placing a specific focus on interoperability is the proposed system of Paci, Ferrini, Musci, Steuer, & Bertino (2009) referred to as Multi-factor Identity Verification (MFV). Under this system the paradigm of collaboration and interoperability aims to be reconciled into one system. In addressing the collaborative efforts of digital identity management systems (DIMs), Paci et al. (2009) present the issue of "naming heterogeneity" which is defined as "occurring in DIMs when various parties involved use different vocabularies to denote identity attribute names" (p.46). These so-called attribute names, by digital standards and also with naming conventions in general, have an almost tangible link to interoperability. Naming heterogeneity is fundamental, just as in language, to facilitating interactivity, and, similarly it is fundamental to interoperability. Using common naming conventions alone may not make for a functionally interoperable system, but the social value of such conventions is worth noting.

Similar, but separate from naming heterogeneity in the MFV, is the basic idea of interoperability across networks. While Paci et al. (2009) cite naming heterogeneity as the crucial factor to interoperability, the key outcome of the MFV as a whole is to provide for unique descriptions of users and their relationships to others. It is information about these relationships which has become of increased importance as the membership in online social networks has grown. The online relationship paradox has gone beyond that of the simple buyer-seller and, in turn, has increased exponentially the need for identifying factors.

The MFV system presents a two phase framework under which the first process, identifying attributes, are presented to the user in order to introduce him/her to another user. The second phase involves a complex verification protocol in which users can match these attributes to trusted parties. This multi-faceted approach is not uncommon in the prevailing literature and, in fact, the approaches themselves highlight many of the important issues raised by competing ideas.

Friedman, Kahn & Howe (2000) underscore the social aspect of identity systems by stating simply, "People trust people, not technology." While Friedman et al. (2000) are of the opinion that individuals are the key to building trust online, he also acknowledges their interdependence: "Online interactions represent a complex blend of human actors and technological systems" (Friedman et al., 2000, p. 36). Through this dichotomy, Friedman et al. (2000) present the concept of value-sensitive design, which calls for constant consideration of human values throughout the creative process of an identity or reputation system. One such value is anonymity; which Friedman et al. (2000) site as having an oppositional relationship to accountability. Because, as he suggests, an increase in accountability generally means a decrease in anonymity, a value-based trust system must place emphasis on finding a balance of the two. As is demonstrated with some of the current reputation systems in place, such as DandyID, the socially focused systems are pacing the expansion of social networks.

A Computational Model

Mui et al. (2002) further the idea of trust and reputation as a chiefly social concept through the presentation of his computational model for trust. This model assumes trust as a foundation to every "face-to-face trade"; *faces* which have become ambiguous not only with the prevalence of digital avatars, but with the facilitation of actual in-person interaction via the internet.

The Mui et al. (2002) computational model defines reputation as "a quantity relative to a particular embedded social network" (p. 4). While this is a novel and potentially useful concept, it is also inherent to the computational model that there is an explicit distinction

between trust and reputation (Mui et al., 2002). This is, at best, another novel approach to identity, but is also one which is divergent from much of the prevailing identity theory. Much of this theory has demonstrated the utility of adhering to a consolidated approach to identity and reputation, or at a minimum, views them as complementary rather than oppositional. This idea has also been supported by the relative success of certain reputation systems currently in place.

In spite of this inconsistency, the computational model still recognizes the primary concern for privacy and anonymity in reputation systems. This, as Mui et al. (2002) posit, is particularly true in the case of naming conventions; specifically in the use of pseudonyms. It is proposed that resilient pseudonyms are crucial to the computational model as they disincentivize misbehavior via the threat of negative reputational consequences.

An Augmented Social Network

The proposal of an integrated online identity, as we have seen, is not new. Not even the premise of an interoperable identity system for social networks is completely novel. Jordan, Hauser & Foster (2003) for example, in their presentation of the Augmented Social Network (ASN), delineate three critical objectives which would facilitate identity and trust online: (1) creating an internet-wide system which enables efficient and effective knowledge sharing, (2) establishing a persistent online identity, and (3) enhancing the ability of citizens to form relationships and self-organize (p. 1). These critical elements are in step with several of the other systems studied, but are of particular interest to this paper because of their emphasis on online socialization. Even more specifically, the research of Jordan et al. (2003) can succinctly be stated as the "creation of online citizenship for the Information Age."

The ASN represents a departure from the previously mentioned NSTIC, but there is a clear relationship between the two. The similarities between the ASN and the so-called "identity ecosystem" are evident. One glaring similarity is the acceptance of an incremental, broad-scale implementation. Both the ASN and the identity ecosystem seek to utilize cross-sectorial inputs (public and private). This crossover in identity and reputation proposals is significant not only

because it brings us closer to a consensus with regard to identity, but more so, because it helps to recognize that the consensus is the goal of online identity.

Digital Footprints

Pew (Madden, Fox, Smith, and Vitak, 2006), one of the leading organizations on internet research, provides some of the most informative statistics and commentary on online identity via its publication on Digital Footprints. Most poignant is its succinct byline of "online identity management and search in the age of transparency" (Madden et al., 2006). Madden & Smith (2010) further identify this idea of transparency in Web 2.0 as the "status quo" in the social networking world. The emergence of transparency as a key to online socialization can be said to have many implications for privacy and anonymity online and the Pew research shows that many people have softened their assumptions of internet privacy (Madden et al., 2006). However the research also shows that there continues to be an expectation of control over personal information in online social networks. This brings us to an important point, as Madden & Smith (2010) go on to emphasize, which is the paradoxical relationship of online privacy and the control of data. With ever-increasing amounts of data available online, the paradox has never been more tenuous. What serves to be particularly informational to the conceptual framework proposed herein is the acceptance of the so-called "beautiful chaos" which embodies the internet and the rejection of our old notions of privacy. Madden & Smith's (2010) ideas, as they pertain to social networks such as Facebook, certainly point us in this direction but leave us with few potential solutions which actually harness online data as a legitimate tool for enhancing personal privacy.

Digital Identity Interoperability and eInnovation

Palfrey & Gasser (2007) present some of the most contemporary theories for and solutions to digital identity interoperability. Much of the resistance to attempts at interoperability has been due to a reluctance to share data – both from a business standpoint and a privacy standpoint.

Palfrey & Gasser's (2007) argument on this subject couldn't be more contrarian in this regard: they posit that digital interoperability – via data sharing – would lead to more secure, more private, and efficient identity management. The larger implications of his theory, however, lie in its relation to innovation – or what they term "eInnovation." Palfrey & Gasser (2007) evoke the aforementioned premise of Madden & Smith (2010) with regard to the control of data. The acceptance of ever-expanding data inputs can, according to Palfrey & Gasser (2007), not only be harnessed to support identity management, but can push technological innovation itself. It is this type of eInnovation which can serve to bridge the gap between public interest and private interest in online identity management. And it is here that we see the underscored importance of collaboration. With what can more easily be viewed as a shared interest, clearer roles can and should be defined for online stakeholders: the government, the private sector, and the individual users of online services.

The Laws of Identity

The so-called "laws of Identity," are Kim Cameron's (2005) attempt at establishing a set of foundational rules for future identity and reputation systems. While his work has proven to be seminal in many respects, the laws laid out have not been accepted wholesale in the current digital identity market because of the constant evolution of online socialization. The focus on conducting business online is, again, acknowledged for its importance but, for the purposes of this research and in order to embrace the trends of the internet, has proven to be only a partial solution. This said, the broader scope provided by Cameron (2005) is relevant still to any proposed conceptual framework. One such informative aspect of Cameron's (2005) work is the pervasive nature of an identity metasystem. This system, like the NSTIC's identity ecosystem, is inherently inclusive of a multi-faceted approach to identity. In Cameron's words, "a single, simplistic identity solution as a universal panacea is unrealistic" (p. 3). And from a practical standpoint, Cameron (2005) cites the impossibility of any such universal system being at all enforceable across international borders. This is indicative of a greater need for collaboration in the development and fortification of online identity and reputation management.

National Strategy for Trusted Identities in Cyberspace (NSTIC)

The U.S. government has attempted to take a proactive role in protecting the rights of its citizens online. One of the guiding principles of the NSTIC is to ensure that any identity solutions being implemented online be privacy enhancing and voluntary. The NSTIC also identifies the divergent relationship between online and offline data collection as it pertains to privacy. "The offline world having structural barriers to privacy," (p. 11); which is exemplified via the use of data trails such as in the tracking of driver licenses. Online identity solutions, according to the NSTIC, should preserve these "positive privacy benefits, while mitigating the negative privacy aspect (Obama, 2011)." While the NSTIC certainly paves the way for a successful identity ecosystem, there is a clear philosophical divergence from contemporary research when it comes to dealing with data. As the NSTIC perpetuates the idea of data minimization, researchers like Palfrey & Gasser (2007) support the unrestricted free-flow of information; with the caveat of it being in a controlled atmosphere. On the surface, these ideas couldn't appear further from reconciliation. But when examined in context, it is precisely this polarization which would support the idea of an identity ecosystem. Multiple stakeholders with varying interests will result in a competition for, and consequently, lead to a maximization of privacy and interoperability in an online identity system. Under such a system, privacy enhancing attributes can also bolster interoperability. These effects can be achieved through one identity metasystem with multiple actors operating under a shared value system.

V. Key Themes

Identity Theory and Practice: A Crossroads

How do we reconcile the different schools of thought represented in the theory of online identity? What is actually being implemented in the practice of online identity? For that matter, how do we reconcile the differences within theory and practice respectively? Here it is important to place the many approaches and theories to online identity in a specific context. The foundations of this context can be defined within the scope of the approaches to identity

that facilitate and/or utilize interoperability, online socialization, privacy and anonymity. Using these concepts as a guide, the review of identity literature and identity systems currently in place were examined in detail and the traits of each were outlined. However, in order to move toward a workable conceptual framework, even further contextual refinement is required. In the following findings and conclusions, we recall back to the dimensions of identity. For each of the dimensions, a reconciliation of theory and practice will be embodied by its conceptual strong points and presented as part of a conceptual framework.

Toward a Conceptual Framework

Given their theoretical nature, many of the findings posed in the prevailing academic works have not necessarily been tested in the marketplace, but have certainly had an influence in the development of identity theory. The literature review conducted helps us to recognize many of the reoccurring themes in the contemporary research and also serves as a juxtaposition to (but more interestingly, as a convergence with) the findings in the Reputation Management Table. These convergences, when examined in the context of the dimensions of identity will lead us to a conceptual framework.

Data Dimension

What implications can be gleaned from the research with regard to data? To be sure, there is no shortage of opinions when it comes to the data dimension of digital identity, however, some clear themes emerge as being agreed upon or simply inevitable in the future of the internet. One of the most apparent among these themes is security. Much of the research examined as well as the systems portrayed, recognize security as being central to building trust on the internet. Further, trust has been identified as the catalyst to online interaction (Resnick, 2004). How do these ideas relate to data? Securing any data that is being used to identify people online has clear consequences for the Information Age. Secure identities in cyberspace have long since been championed as a route to a safer internet. Securing data - a broad

concept in identity theory - with the preceding research in mind, must be broken down into specifics should the conceptual framework presented here be of any use to future researchers and developers.

One important factor in bridging the gap between secure data and secure identities is the concept of resiliency. Data, in the digital age, is not always accurate and this fact alone demonstrates why all data should have a strong correlation to an individual user. While this point may seem counterintuitive, it holds true as resilient data - whether accurate or not - boosts the value of honest usership on the internet. This notion is poignantly demonstrated through the use of so-called "cheap pseudonyms" in systems such as eBay's. While eBay is clearly flawed in its inability to "punish" repeat offenders who can create an unlimited number of pseudonyms on its site, it does have some noticeable success in allowing honest users to separate themselves by giving off the perception of greater credibility through their experience. This said, eBay has become the antithesis of resiliency online and, despite its commercial success, should be recognized as such. New and emerging systems should account for the shortcomings of systems like eBay; specifically trying to solve the problem of resiliency.

One possible means of solving the resiliency issue is data sharing. Paci et al. (2007) support an approach of open data sharing, where multiple systems can utilize and share mass-disclosed information and data. This approach is in stark contrast to Cameron's (2005) idea of minimal disclosure for constrained use – which holds that the identity solution which discloses the least amount of identifying information and best limits its use is the most stable and long-term solution. The conceptual framework proposed abandons any attempt to reconcile these polar opposite ideas and instead only suggests that one may be better suited in the ever-expanding online social atmosphere. Attempts to resist data sharing online have been all but futile in the internet age and, with the expansion of online social networks, have steadily been abandoned altogether. Given that online social networks and the general socialization for the internet do not appear to be passing trends, the ineffectiveness of attempts to limit data sharing seems all the more apparent. As Paci et al. (2007) suggest, it is much more practicable to harness open identity sharing in online identity development as individual users continue to share more data.

The time is not far off when we will have an adult population that has not known a life without the presence of the internet and online socialization, and as more data is made available online, digital identity providers would be remiss in opposing the power of open data sharing.

Accepting this approach to data as a foundation to online identity will, in turn, allow for a more collaborative, and specifically, interoperable approach; an approach which can then come full circle to the notion of transference-based trust. An increase in the usership – as well as in scope – of the internet has led to an expansion in the services offered online; many of these services have been embodied in the form of a social network. Just as the presence of data online has expanded precipitously, so too has the influence of social networks. Thus, it is the acceptance of these trends, rather than a resistance to them, that will more likely prove effective in online identity management. Cooperation between social networks in an interoperable identity system will allow for the inherent trust of those networks to be shared and personified in the individual user (i.e. transference-based trust). For all intents and purposes, open data sharing will allow for transference-based trust across networks and, consequentially, will lead to more secure identities in cyberspace.

Use Dimension

With a better understanding of the role of data in identity management, we now have some perspective on the purpose of a conceptual identity management system and a context in which it will operate. Data, among internet marketers, has come to be closely associated with leverage in online business – or stated more bluntly, "data is power." As shown in the analysis of the data dimension of identity, the internet has been flooded with data and attempts to control such data are, essentially, attempts to control power. Systems, whether implemented (as in eBay) or proposed (as in Cameron (2005)) which have tried to centralize power vis-à-vis data, have generally been met with resistance from users. This only follows naturally in a data-driven environment as in the internet, and more specifically, in online social networks. So then, for the purposes of a conceptual framework, we can favor a more decentralized approach – chiefly through the empowerment of the individual user. Shifting power to the individual is not

only practicable given the flow of data and information on the internet, but is also a common thread in much of the prevailing identity theory discussed here. By many accounts, crowds (groups of users) possess much of the power in social communities and, not coincidentally, have a stake in supporting online citizenship which would increase trust and social participation. While interests may vary across social networks, online citizenship has the potential to be ubiquitously beneficial. Here, we begin to see the convergence of several trust-related concepts in cyberspace. Online citizenship, digital footprints, digital identity, and online reputation can all be viewed as means to one end: the creation of an identity ecosystem.

Perhaps stated most eloquently, the NSTIC (Obama, 2011) compares the identity ecosystem to ecosystems existing in nature, suggesting, "it will require disparate organizations and individuals to function together to fulfill unique roles and responsibilities" (p. 21). To take this analogy a step further, much of the information extracted in the research here reinforces the idea of organic and adaptable systems for identity. Systems with rigid and immovable regulations which have no capacity for interoperability are almost unanimously discounted among contemporary researchers. Consistent with an approach to data sharing, identity system providers must work in collaboration if a harmonious identity ecosystem should be established. Once again, why is the establishment of an identity ecosystem so imperative? In summary, an identity ecosystem is needed if the current problem of identity in silos is to be overcome. Siloed identity systems fall short when confronting the larger problems of identity online; this is largely due to an incapability to achieve interoperability.

Methodology Dimension

In returning to the identity management table, we see that each of the methodologies to identity have been implemented in similar contexts. Previously, the successes and failures of the varying systems were discussed and although some patterns can be identified, it is not possible to completely dismiss any of the methodologies as being ineffective solely based on the sample selected. But the analysis of the methodologies can be informative particularly given the contextual research previously discussed. In specific, it helps to characterize how the

evolution and expansion of the internet and social networks has posed several problems in implementing the various methodologies to identity. The problem of scalability is one of the more apparent issues presented. The certification and authentication methodologies do have their supporters in identity theory, but many have become marginalized in recent times as both tend to be resource-intensive in an environment where resources are increasingly at a premium. Certification and authentication also generally share the problem of interoperability. Issuing a "credibility certificate," for example, or further trying to authenticate such certificates becomes more and more problematic as diverse user groups with diverse interests emerge. In this respect, these methodologies are antithetical to supporting growth in online social networks.

The use of a reputation ranking methodology has been criticized greatly in identity management, in large part because it is the most frequently utilized. That said, the intentions of the reputation ratings methodology – as they pertain to empowering the individual user –are viable in addressing the issues of scalability. At a fundamental level, the empowerment of the individual should be a focus for any identity system; this is the main contribution of a reputation ranking as we know them today. Systems such as eBay's are naturally susceptible to gaming and tend to incentivize adverse behavior in their communities. This being the case, a traditional reputation rating system seems all the more unfeasible in attempting to match in scale the growth of social networks.

This leads us to the methods of profiling and linkage – the two most novel and underutilized methods. Profiling systems, as in the systems which preceded it, tend to be resources-intensive and therefore, seemingly non-scalable in the realm of interoperability. However, one of the aforementioned prerequisites for interoperability – resiliency – is at the forefront of a linking system. A third party (actually an infinite number of parties) contributing to a trust profile is not only scalable in theory, but also is capable of utilizing transference-based trust. The credibility, or the trustworthiness, of communities which establish varying degrees of trust can collaborate by contributing to the larger identity ecosystem. By transferring trust inherent to these communities to the identity ecosystem, trust would be enhanced on a larger scale.

Again, the idea of an ID profile online is not new, but due to the expansion of the internet and an ever-increasing number of profiles being used, online IDs have only compromised reputation management on the internet by instituting homogenized, unquantifiable, and siloed identity systems. Clearly a crossroads has been reached in the theories of centralized and decentralized identity management and the conceptual framework proposed here makes no attempt to define a clear-cut best practice between the two. In order to "empower the individual user" one would think that a decentralized system would yield the best results. Conversely, in order to overcome identity in silos by consolidating identity systems, a centralized identity system seems the logical solution. It is here where we can look to an alternate methodology for a solution.

Linkage, with its intention to describe connections between people, has been a largely untested approach which has come to fruition specifically due to the growth of online social networks. This, we can deduce, has been to address the issues of scalability and interoperability in identity systems. Here we can poignantly turn to the example of social network giant Facebook in its collaboration with Couchsurfing.org. The Couchsurfing found that by linking its users to the larger, possibly more trusted, social network that they could increase the trust of their own community – transferring the trust of Facebook users to Couchsurfers. Their success (growth) begs the question: Is this tactic scalable and is it repeatable? Based on the research here, it is proposed that the answer to both questions is in the affirmative. Linking trusted (or even not-so trusted) communities together really has no limits and, more importantly, seems to bare the seeds of an identity ecosystem. If more and more online communities linked to a larger network of communities, individual users would consequently be more attached to an interoperable online identity. That is to say that more connections to more users will, in turn, make individual users more beholden and more accountable to their reputation and help to identify themselves across the internet.

From here, we return to the notion of a profiling methodology. If more online social networks were to begin linking their users with those of other networks (decentralizing identity) how would the individual users' trust be perceived or portrayed to the internet at large if an infinite

amount of connections were being made? A more resilient and quantifiable system may also present a (centralized) identity profile which could serve as a "common language" for reputation management. A profile which could generally be recognized by internet users could provide descriptive characteristics for those users inter-linked in the identity ecosystem. With this, a centralized and decentralized system can work simultaneously and offer a scalable and interoperable solution.

Infrastructure Dimension

Specifically how this profiling-linking hybrid should be embodied will have to be left to those with the means to implement such a system. However, from a conceptual standpoint, it is supported here that the future systems will have to embrace similar methodologies in order to enhance trust among their users. Nonetheless, with an established methodology dimension in the conceptual framework, we can look to the infrastructure requirements such a system would have.

Using unique technologies and naming conventions is antithetical to interoperability (the online equivalent of a language barrier). So then, the conceptual framework should use consistent technologies (e.g. ID profiles) across the identity ecosystem. In more specific terms, the identity ecosystem should be supported by a network of relying parties that would not only contribute to reputation management, but also rely upon it. This mutual exchange is at the core of interoperability, which will serve the individual user through his or her own empowerment.

Recalling the proposed use for data in the conceptual framework, open data sharing is meant to provide users with as much information as possible regarding fellow users. Data alone, however, will not accomplish this. Instead, data must be presented in a way that is meaningful to the user. In this respect, the individual user profile – which is derived specifically from linking to other social networks – will allow users to gage the trustworthiness of other users (external) but also allows the user to gage their own trustworthiness (internal) as perceived by

others. This has the potential for developing a mutual understanding of identity which would further the notion of the identity ecosystem.

Further, the user profile as it pertains to the systems infrastructure should be constructed with a value-sensitive design. As the proposed system is chiefly concerned with social networks – and therefore concerned with social interaction involving real people – the value of those people should be weighted heavily in the infrastructure. Human integration through a value-sensitive design is, by definition, certain to be inclusive rather than exclusive of the human element which is central to the online experience. What values should be incorporated? The overarching goal of an identity system is to increase trust; so the values incorporated in the system should behave in accordance with this. In concert with the theories discussed, those chief values are security, privacy and anonymity. Each of these values, when examined independently, could arguably have conflicting and inverse relationships with one another; however, an open data system with a resilient user ID has the potential to enhance each of them. A secure system, which would typically be viewed as a closed system, can offer more security to its users by presenting the greatest amount of data available pertaining to other users while allowing them to control the amount of data being shared about themselves. This would have the effect of empowering the user to make decisions about their social interactions and also to make themselves more credible in the eyes of those with whom they are interacting.

Through the development of online citizenship within the internet ecosystem, privacy and anonymity will likely increase in their importance. Again, an open data sharing system may seem antithetical to privacy and anonymity – but this does not have to be the case in evolving identity systems. Having more identifying factors (more links) does not mean less privacy. In fact, it means just the opposite. Currently, users create a new profile for each new community they want to join – allowing more and more access to their personal information. With a resilient and interoperable user profile, the credibility of their profile alone could grant them access to new services online while minimizing the spread of their personal information and increasing privacy.

There is a similar effect on anonymity. Although user profiles would be resilient and "follow" the user, the user profile itself serves as an extension (or avatar) of the user which would still allow for a certain degree of anonymity via separation from the actual person socializing online. That anonymity is crucial to facilitating online authorship and interaction that can benefit the user and the community (e.g. support groups and discussion forums). The maintenance of privacy and anonymity is central to trust building and, therefore, to value-sensitive design.

Clearly, the infrastructure dimension of identity would prove to be the most complex when designing an identity system, so – just as in the conceptual framework – the dimension laid out here can only serve as a foundation.

With these key themes identified regarding the dimensions of identity, what sort of semblance can be formed between them? By way of conclusion, the following section attempts to bring together the dimensions of identity in such a way that would ultimately support the identity ecosystem.

VI. Conclusions

The Dimensions of Identity and Interoperability

The dimensions of identity, if implemented piecemeal, may have little impact on the interoperability of an identity management system. As fundamental, connected units of digital identity, however, they have the potential to not only integrate but to mobilize the stakeholders of online identity. While they should not be viewed as comprehensive, the dimensions described here represent a strong foundation for combating the current issue of identity in silos. Should a preponderance of online stakeholders adopt these dimensions as a basis for identity management, the identity ecosystem could help to perpetuate interoperable identity through further developing the characteristics of the dimensions of identity.

Characteristics of the Dimensions of identity

In characterizing the most important implications of the dimensions of identity, we can develop the proposed conceptual framework. Those implications which have been laid out in the preceding sections will now be summarized for the sake of clarity and, specifically, to address the question:

What factors are most important in designing an interoperable online reputation management system that will enhance the trust of its users while accommodating the rapid growth of social networks?

In addressing these questions, we return to the design theory in Figure 1. The kernel theories taken from our data analysis have led to the identification and characterization of the dimensions of identity. Using the ultimate goal of interoperability in an identity system (in addition to the collected data), a theory on the desired characteristics of these dimensions is now more easily extrapolated. More specifically, a conceptual framework composed of the four dimensions of identity should incorporate the following:

Data Dimension - data should (1) be resilient, (2) be secure, and (3) allow for open-data sharing.

Use dimension – context of use should be that which (1) empowers the individual user, and (2) is broadly adoptable.

Methodology dimension – methods should (1) be scalable, and (2) utilize a linkage/profiling methodology

Infrastructure dimension – foundational factors should (1) use consistent technology, (2) utilize internally and externally perceived identity, (3) support a value-sensitive design, and (4) garner trust and maintain anonymity.

The characteristics of the dimensions above serve as a conceptual framework for an interoperable identity management system. Based on the data analyzed, these dimensions are the most important design factors if interoperability is the goal. Further, as this research was based on the assumption of increased sociability (online social networks) on the internet, the notion of online interoperability becomes a more clearly evident outcome. The characteristics of the dimensions of identity were formulated with this outcome in mind and represent a foundation for future development.

This paper also set out to establish a greater understanding of the role of digital identity in the future of the internet and how developers of identity systems could address its challenges. So how does the newly defined digital identity influence future identity management systems? While this is nothing short of a complex question, it is posed that the conceptual framework outlined here can serve as a starting point.

The four dimensions of identity (data, use, methodology, and infrastructure) help to define the ever-evolving notion of digital identity and its place on the Web and in real life. These dimensions allow for a more comprehensive understanding of how digital identity relates to interoperable and global collaboration online. In harnessing these concepts, designers of identity management systems should be able to create software that will not only inhibit detrimental behavior online, but also facilitate online socialization.

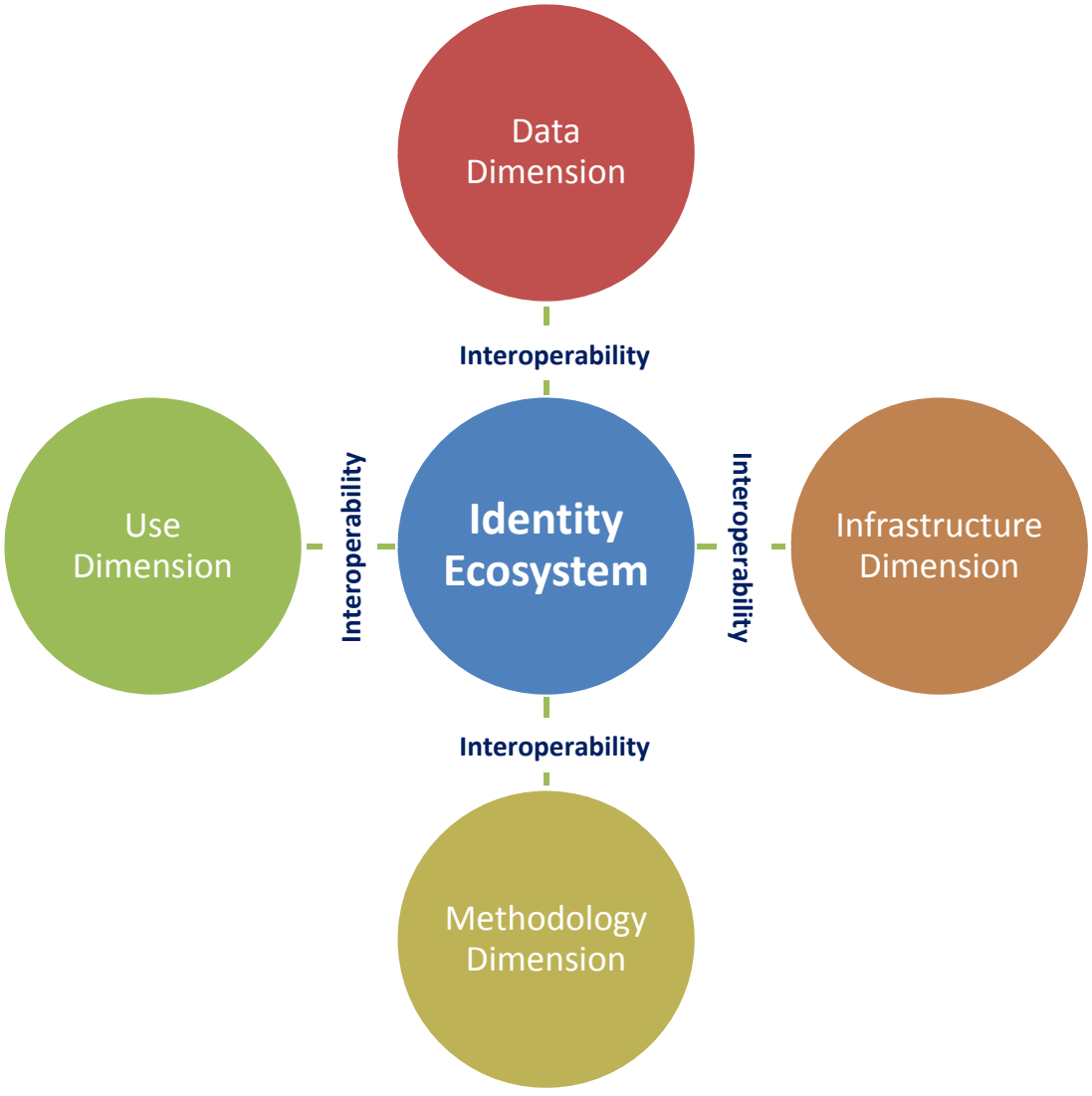
In once again referring to the design theory in Figure 1, we see the Identity Management Design and the Identity Ecosystem as the ultimate components of the design theory. Given that there is more to the design of an interoperable identity system beyond the dimensions of identity, these final two components must be addressed. More specifically, it is the relationship between these components that will help to inform future research and development.

Identity Management Design & the Identity Ecosystem

Over the course of this research, the link between its central theme – interoperable online identity – and the identity ecosystem has drawn closer and closer. It is posed here that (if an

identity ecosystem is the eventual goal) the two are codependent. To again evoke the metaphor of an ecosystem existing in nature, we should recall that ecosystems are defined by the network of interactions among and between organisms and their environment. These interactions are central to the survival of the ecosystem, just as interoperability is to the identity ecosystem. Interoperability itself must serve as a link for the dimensions of identity in order for a sustainable identity ecosystem to be established. Figure 2 below demonstrates this relationship.

Figure 2. Interoperability in the Identity Ecosystem



Ultimately, the Identity Ecosystem can only be created with the cooperation of many individual actors in the online community. No single company or government could or should be the keeper of such a system. There have already been significant efforts to establish online identity and the forming of an ecosystem is underway. That is why – in its developmental stage – the future of the identity ecosystem is so important. There is a powerful and impending argument for the development of the identity ecosystem in the immediate future and a similarly compelling argument for posterity's sake.

LIMITATIONS

As we have seen, Palfrey & Gasser (2007) take a highly in depth look at one of the core issues of this thesis: interoperability. Like Obama (2011), they suggest that there is no all-inclusive solution to the problem of online identity and reinforce the idea that multiple players will have to contribute to a larger identity ecosystem (or as they refer to it, a metasystem.) Most poignantly, they suggest that the incentives for market players are largely aligned in their current state, but may diverge as technological and market developments progress and also that the largest potential pitfall is a breakdown of collaboration among stakeholders (Palfrey & Gasser, 2007).

Given these potential pitfalls, there are some obvious limitations for future designers of identity systems. The most notable, and that which has been reinforced throughout this paper, is the tendency of systems to present themselves as a panacea in the field of reputation management. In a highly competitive, profit-based market, this mind-set may be difficult to avoid. That is, a collective and collaborative approach may prove too cumbersome with the internet as we know it today.

A microcosm of this limitation is represented in any gaps in communication between identity management providers. As Palfrey & Gasser (2007) suggest, collaboration (via communication)

is a major potential pitfall to identity today and given the alignment of interests in the current market, there arises some urgency if any such collaboration were to occur. Suggesting that the creation of a cooperative identity ecosystem is a time-sensitive issue is a clear limitation. With so many online stakeholders, to see any significant developments in the online ecosystem may, in fact, not even be realistic.

FUTURE RESEARCH AND PRACTICAL IMPLICATIONS

It is keeping these limitations in mind which can help us to identify a course of action for future research. Outside of exploring ways to develop and improve the conceptual framework presented, the urgency of exploring ways to improve communication and collaboration between online stakeholders becomes more apparent. One such avenue of research could be to study (as was started by the NSTIC) the role of governments in creating an online identity ecosystem. Traditionally, government has served to represent the shared interest of its people and the modern internet represents one of the greatest shared interests we have ever seen. Online identity is a global issue. Governments, alongside private corporations, should therefore, research ways to increase collaboration on a global scale when discussing matters of online security. As the internet has evolved from a highly individual user experience to an almost ubiquitous presence in our lives, future research should recognize the massive influence of the internet while balancing it with the fact that behind each computer screen is a human being.

Appendix A - References

Ba, S., (2001). Establishing online trust through a community responsibility system. *Decision Support Systems*, 31, 323–336.

Backhouse, J., (2006). Interoperability of identity and identity management systems. *Datenschutz und Datensicherheit,* 30(9), 568-570.

Basu, A., & Muylle, S. (2003). Authentication in e-commerce. *Communications of the ACM*, 46(12), 159-166.

Bhattacharjee, R. & Goel, A., (2005). Avoiding ballot stuffing in eBay-like reputation systems. *Proceedings of the 2005 ACM SIGCOMM workshop on economics of peer-to-peer systems,* 133-137.

Blitstein, S., (2009). Digging Deeper Into DandyID. [Web log comment]. Retrieved from http://gigaom.com/2009/07/28/digging-deeper-into-dandyid/

Bouman, W., de Bruin, B., Hoogenboom, T., Huizing, A. & Jansen, R., (2007). The realm of sociality: notes on the design of social software. *Sprouts: Working Papers on Information Systems*, 8(1), 1-25.

Brown, J. & Morgan, J., (2006). Reputation in online markets: some negative feedback. *IBER Working Paper, University of California, Berkeley*, 1-30.

Cameron, K., (2005). The laws of identity. *Microsoft Corporation*, 5/12/2005.

Deaux, K., (1993). Reconstructing social identity. *Personality & Social Psychology Bulletin*, 19(1), 4-12.

Duan, H. & Liu, F., (2012). Building robust reputation systems in the e-commerce environment. In Proceedings of *TrustCom*, 2012, 326-333.

Friedman, B., Kahn, P. & Howe, D. (2000). Trust online. *Communications of the ACM*, 43(12), 34–40.

Gordijn, J. & Akkermans, H., (2001). Designing and evaluating e-business models. *IEEE Intelligent Systems,* 2001, 16(4), 11–7.

Hampton, K., Sessions Goulet, L., Rainie, L. & Purcell, K., (2011*).* Social networking sites and our lives. Technical report, Pew Internet & American Life Project, 2011, 1-85.

Hansen, M., Schwartz, A. & Cooper, A., (2008). Privacy and identity management. *IEEE Computer Society*, 6(2), 38–45.

Jensen, C., Davis, J., & Farnham, S., (2002). Finding others online: reputation systems for social online spaces*. CHI 2002 Conference, Human Factors Computer Systems, ACM Press,* New York, 447–454.

Jordan, K., Hauser, J. & Foster, S., (2003). The augmented social network: building identity and trust into the next- generation internet*. First Monday*, 8(8).

Lim, S., Cho, H. & Rivera Sanchez, M., (2009). Online privacy, government surveillance and national ID cards. *Communications of the ACM*, 52(12), 116–220.

Madden, M. & Smith, A., (2010). Reputation management and social media. Technical report, Pew Internet & American Life Project.

Madden, M., Fox, S., Smith, A. & Vitak, J., (2007). Online identity management and search in the age of transparency. Technical report, Pew Internet & American Life Project.

Mui, L., Motashemi, M. & Halberstadt, A., (2002). A computational model of trust and reputation. In Proceedings of the *First International Joint Conference on Autonomous Agents & Multiagent Systems (AAMAS)*.

Obama, B., (2011). National strategy for trusted identities in cyberspace. Washington D.C: The White House.

Organisation for Economic Co-operation and Development (OECD), (2009).The role of digital identity management in the internet economy*:* a primer for policy makers. *OECD Digital Economy Papers*, No. 160, 1-21.

Osterwalder, A., Pigneur, Y. & Tucci, C., (2005). Clarifying business models: origins, present and future of the concept. *Communications of the Association for Information Science (CAIS)*, 16, 1-25.

Paci, F., Ferrini, R., Musci, A., Steuer Jr., K. & Bertino, E., (2009). An interoperable approach to mulitfactor identity verification. *IEEE Computer Society*, 42(5), 50-57.

Palfrey, J. & Gasser, U., (2007). Digital identity interoperability and eInnovation. *Berkman Publication Series, Harvard University*. Retrieved from http://nrs.harvard.edu/urn-3:HUL.InstRepos:2710474

Resnick, P., (2004). Reputation systems. *Communications of the ACM*, 4 3(12), 45–48.

Resnick, P. & Zeckhauser, R. (2001). Trust among strangers in internet transactions: empirical analysis of eBay's reputation system. *Advances in Applied Microeconomics*, 11, 1-26.

Sökefeld, M., (1999). Debating self, identity, and culture in anthropology. *Current Anthropology*, 40, 417-447.

Tajfel, H., (1978). Differentiation between social groups: studies in the social psychology of intergroup relations. London: Academic Press.

Tapscott, D. & Williams, A., (2006). *Wikinomics: How mass collaboration changes everything*. New York: Portfolio Trade.

Ubois, J., (2003). Online reputation systems. In *Release 1.0*, 21(9), 1-35.

Wall, D., (2007). Cybercrime: the transformation of crime in the information age. Cambridge, UK: Polity Press.

Walls, J., Widmeyer, G. & El Sawy, O., (1992). Building and information system design theory for vigilant EID. *Information Systems Research*, 3(1), 36–59.

Whittemore, N., (2011, May 7). Why the internet debate could restart the culture war. [Web log comment]. Retrieved from www.http://technology.inc.com.

Appendix B - Websites

Cisco Identity Services Engine - http://www.cisco.com/en/US/products/ps11640/index.html

Couchsurfing - https://www.couchsurfing.org/

DandyID - www.dandyid.org/

Web of Trust - http://www.mywot.com/

eBay - www.ebay.com/

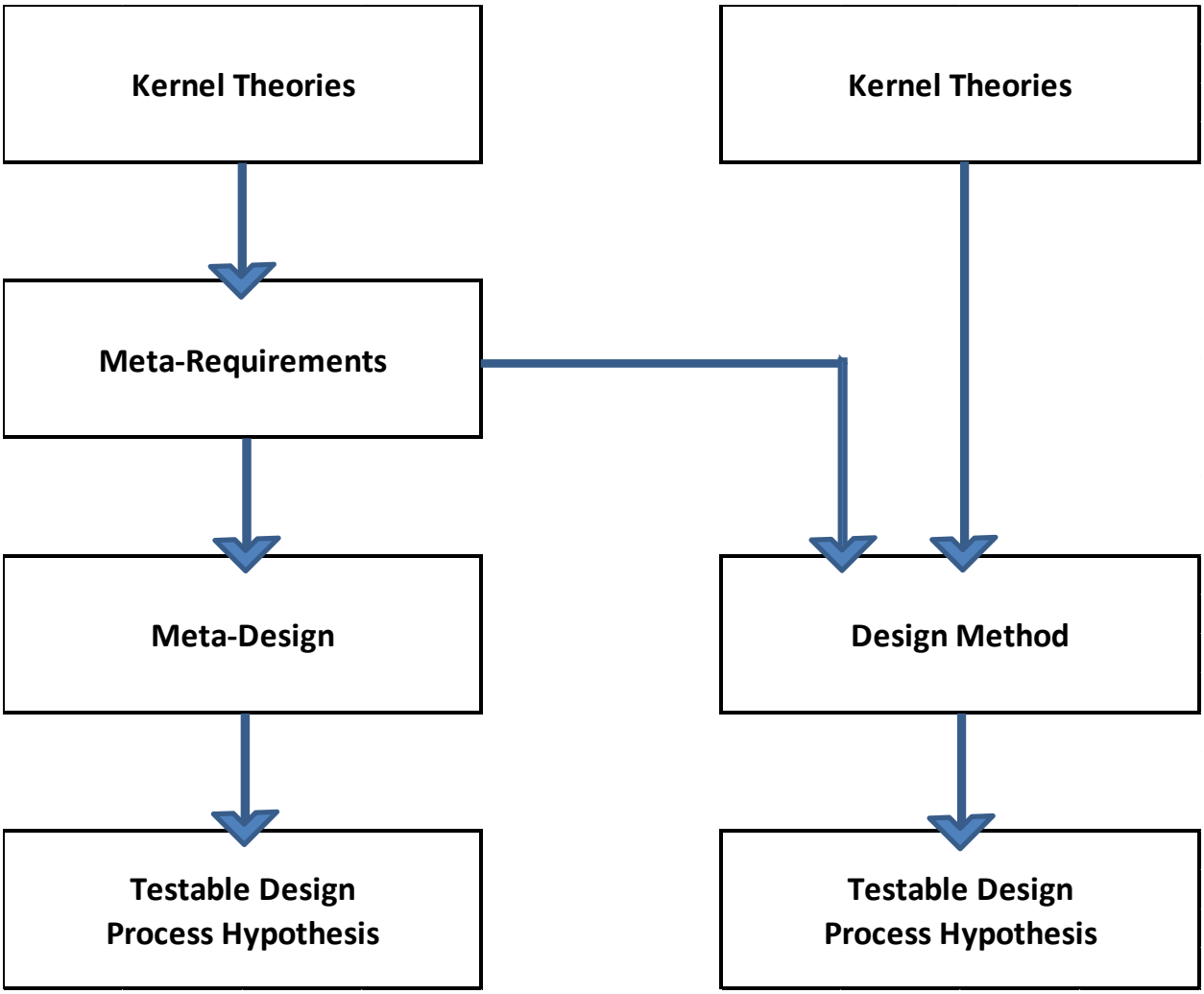
MyID.is – http://myid.is/

OpenID - http://openid.net/

VeriSign Identity Protection Services - http://www.symantec.com/verisign/vip-authentication-service

Windows Live ID - https://accountservices.passport.net/ppnetworkhome.srf

Appendix C –Design Theory Structure (Walls, Weidmeyer & El Sawy, 1992)



Appendix C (cont.) – Design Theory Structure (Walls, Weidmeyer & El Sawy, 1992)

Components of an Information Design Theory

Design Product	
1. Meta-requirements	Describes the class of goals to which the theory) applies.
2. Meta-design	Describes a class of artifacts hypothesized to meet the metarequirements.
3. Kernel theories	Theories from natural or social sciences governing design requirements.
4. Testable design product hypotheses	Used to test whether the meta-design satisfies the meta-requirements.
Design Process	
1. Design method	A description of procedure(s) for artifact construction.
2. Kernel theories	Theories from natural or social sciences governing design process itself.
3. Testable design process hypotheses	Used to verify whether the design method results in an artifact which is consistent with the meta-design.