European Journal of Information Systems (2014) 23, 69–83

www.palgrave-journals.com/ejis/

EMPIRICAL RESEARCH

Organizational identity and information systems: how organizational ICT reflect who an organization is

Michael Tyworth

Penn State University Park, U.S.A.

Correspondence: Michael Tyworth, Smeal College of Business, The Pennsylvania State University, 430 Business Building, University Park, PA 16802, U.S.A.
Tel: 1-814-865-2224;
Fax: 1-814-863-7067;
E-mail: mjt241@smeal.psu.edu

Abstract
The work reported here contributes to our understanding of organizational identity regarding its influence on organizational action related to the development of information and communications technologies (ICT). The empirical basis of this work comes from case studies of integrated criminal justice information systems (IJIS). IJIS are organizational and technological ensembles created to facilitate inter-organizational information sharing among criminal justice agencies. The focus of these case studies was to examine how organizational identity shapes organizational ICT. This research found that organizational identity shapes an organization's ICT-related processes and is reflected in the material configurations of an organization's ICT; and that organizations with different identities exhibit those differences in their ICT. Three implications of this research are that organizational identity serves as both an enabler and constraint on organizational ICT development; organizational identity commitments will likely serve as a barrier to large-scale integration of different organizations' systems; organizational identity is relatively static and difficult to change.
European Journal of Information Systems (2014) **23,** 69–83. doi:10.1057/ejis.2013.32; published online 19 November 2013

Keywords: green is; organisational & inter-organisational initiatives; social/organisational aspects of is

Introduction

The social features of an organization play an important role in shaping the form and features of its information systems (IS). Culture, norms, values, rules, and attitudes of an organization play an important mediating role in system development, implementation, and outcomes (Kling *et al*, 2005; Leonardi & Barley, 2010). For example, technologies that are misaligned with a firm's culture and norms can go unused or even actively resisted by employees (Orlikowski, 1993; Markus, 2004). Legitimacy pressures can influence managers to adopt new, 'fashionable', technologies independent of actual technological performance (Wang, 2010). Information technology (IT) projects often fail as a result of a lack of stakeholder buy-in and top management commitment (Luna-Reyes *et al*, 2005). Understanding and managing the social dynamics that surround organizational technology is critical to achieving successful technology outcomes.

In turn, organizational IS have a mediating influence on the social features and practices of organizations. Adoption of an enterprise resource planning system implies a certain commitment by the organization to standardization and integration of business practices and processes (Li Da, 2011). At hospitals and clinics where there is a significant IT presence, nurses and

Received: 14 January 2011
Revised: 01 August 2011
2nd Revision: 06 February 2012
3rd Revision: 28 June 2012
4th Revision: 15 June 2013
5th Revision: 01 September 2013
Accepted: 30 September 2013

physicians often are no longer just responsible for diagnosis and patient care, but also for data entry and, in some cases, technical support (Ash *et al*, 2004). Educators have had to adjust their teaching styles, modes of interaction and even expectations of classroom decorum in response to the increased presence of technology in the classroom (Baldwin, 1998). It is clear that when organizations implement institute technological change, they must also address the attendant social changes associated with the new technology (Markus & Benjamin, 1997; Markus, 2004).

Scholars of IS have extensively explored how IT affects, and is affected by, many different aspects of organizational life. Some of the social aspects of organizational life that feature prominently in the literature include: IT and organizational culture, learning, structure, strategy, and innovation among numerous others (Dewett & Jones, 2001). An organizational social dynamic that is receiving increasing attention in the IS community is organizational identity. An organization's identity is its understanding of who it is and how it is uniquely different from other organizations (Dutton & Dukerich, 1991; Reger *et al*, 1994; Elsbach & Kramer, 1996; Gioia & Thomas, 1996; Dukerich *et al*, 2002; Corley & Gioia, 2004). Organizational identity is a driver of organizational discourse, decision-making, and action in that it acts as a referent for what is appropriate behavior by the organization. For this reason, organizational identity is likely to play an important mediating role in IS development and implementation by acting as a deep structure providing the foundation for higher-level organizational arrangements and technologies (Silva & Hirschheim, 2007).

This research explores two questions: (1) How does organizational identity manifest itself in IS development? and (2) Can the influence of organizational identity on system development be seen in the material configurations and features of the technology? Using Albert & Whetten's (Whetten, 2006) theory of organizational identity a theoretical lens, this research seeks to answer these questions through comparison of two case studies of organizations for whom development and implementation of IS is the very basis for their organizational existence. These organizations, called integrated criminal justice information systems (IJIS), are complex organizational-technological ensembles created to develop technological infrastructures that facilitate inter-organizational information sharing among criminal justice and public safety agencies. IJIS are complex socio-technical systems for which the organizational and technological elements are fundamentally intertwined to the extent that, without both elements, they no longer can be considered IJIS (Fedorowicz *et al*, 2006, 2007; Sawyer *et al*, 2007). For this reason, IJIS are an excellent organizational form in which to study the relationship between organizational identity and the development of IS.

This research makes two contributions. One, this research provides initial insight and understanding into how social and organizational factors influence development initiatives by detailing the ways in which organizational identity influences both technological processes and, ultimately, the material outcomes of system development. Two, this research offers insight to professional practitioners engaged in integrated justice system development by drawing attention to the ways in which their organization's identities facilitate the configuration of some information and communications technologies (ICT), while constraining others. As developers of integrated inter-organizational systems, IJIS developers must pay particular attention to the ways in which organizational and social factors impact their development efforts (Luna-Reyes *et al*, 2005).

This paper proceeds in three parts. The first part is a review and synthesis of the extant literature on organizational identity and ICT and the research domain providing the theoretical and empirical basis for this research. The subsequent section summarizes the research approach and analytical method used in this research and presents the case study data. The last section of this paper discusses the findings and their implications for IS and organizational research and for professional practice.

Organizational identity

Organizational identity has received widespread attention in the management literature. Organizational identity theory describes three dimensions (see Table 1) of organizational identity: the *ideational*, the *definitional*, and the

Table 1 Dimensions of organizational identity

Identity dimension	*Definition*	*Description*
Ideational	The perception of who the organization is; as collectively understood by its members.	The *ideational* component of organizational identity reflected in statements of who the organization is.
Definitional	Central, enduring, and distinctive characteristics of an organization.	The *definitional* component of organizational identity is the attributes that specify how the organization is similar to, and different from, other organizations.
Phenomenological	Organizational identity reflected in organizational discourse.	The *phenomenological* component is organizational discourse related to how the organization must act in order to be consistent with who the organization is.

phenomenological (Albert & Whetten, 1985; Whetten, 2006). The *ideational* dimension of organizational identity is the internal membership's perception of who the organization is. The *definitional* dimension includes the specific features, competencies, and practices of the organization that make the organization unique. Finally, the *phenomenological* dimension is the organization's identity it is instantiated through discourse and organizational action. In other words, an organization's identity is comprised of its member perceptions, its material features, and its actions.

There is debate over the extent to which organizational identity is continually negotiated by the membership (a process) or is an institutionalized organizational feature that functions as an external (a structure) and is currently contested in the literature (Haslam *et al*, 2003; Whetten, 2006). Prior research adopting the former perspective has found that incongruence among an organization's internal identity and external image can initiate shifts in an organization's identity (Dutton *et al*, 1994); organizational change introduces a period of identity ambiguity (Gioia *et al*, 2000); disagreement about an organization's identity among top management can negatively impact firm performance (Voss *et al*, 2006); and that the organizational identities are shaped externally through technological boundary objects (Gal *et al*, 2008). Research on organizational identity adopting the latter perspective has found that: organizational identity acts a reference for strategic behavior (Shrivastava & Schneider, 1984; Merali, 2002; Winter *et al*, 2003); influences interpretation of issues by organizational members during times of change (Gioia & Thomas, 1996); and as a basis for resistance against institutional pressures (Brunninge, 2005).

This duality suggests that organizational identity is structurational; it is both continuously enacted and institutionalized (Ravasi & Van Rekom, 2003; Whetten, 2006). Structuration theory posits that social structures only exist as long as they are continually produced and reproduced through human action, yet they serve to guide and constrain behavior in a self-reinforcing manner (Desanctis & Poole, 1994; Rose, 1998; Orlikowski, 2000; Jones & Karsten, 2008). Thus, organizational identity theory exhibits structurational characteristics in that it accounts for the ways in which organizational identity institutionally resists change and the way it can be changed as a result of both internal and external pressures (Brunninge, 2005; Whetten, 2006).

Organizational identity and technology

Prior work on organizational identity and IT has been relatively limited (Kjaergaard & Gal, 2009). There are two streams of research on organizational identity and IT. The first stream focuses on the ways in which organizational identity influences user behavior. Lamb & Kling (2003) theorized that users' identities, as members of the organizations, are simultaneously informed by, and shape the use of ICT. Speier & Venkatesh (2002) found that the introduction of new systems that were incongruous with the extant organizational identity contributed to user resistance in the form of increased absenteeism and leaving the organization. One implication of this stream of research is that organizational identity influences users' perceptions of, reactions to, and uses of organizational ICT.

The second stream focuses on the impact of organizational identity on organizational action as it relates to technology. For example, Tripsas (2009) found that organizational identity served to limit the types of new products the organization perceived itself as capable of making. The organization studied found it difficult to develop new product lines that were divergent from its entrenched organizational identity as a producer of digital photography technologies. Similarly, Winter *et al* (2003) found that organizations develop websites for external consumption in ways that affirm their internally held identity. Thus, organizational identity served as a referent for system development, even though the technological products were for external customers.

Research setting: IJIS

This research studied policing IS for two reasons. One, ICT are a core component of policing activity, and are central to the criminal justice enterprise (Hoey, 1998; Manning, 2003; Sorensen & Pica, 2005). The modern criminal justice agency often makes use of sophisticated electronic records management systems to track offenders as they work their way through the criminal justice process. A modern police vehicle typically contains an array of information technologies, such as a laptop computer, a mobile data terminal (a dumb terminal connected to a back-end system), and a navigation system. A patrol officer often will have a smart-phone or cellular phone on their person along with their police-issue radio.

Two, criminal justice domain is institutionally complex. The U.S. criminal justice system employs a federalist model with authority decentralized and distributed to the local level. There are over 17,000 state and local law enforcement agencies in the United States (United States Department of Justice Office of Justice Programs Bureau of Justice Statistics, 2007), the majority of which have their own chain of command, funding mechanisms, organizational structures, and technological infrastructures. Though, in recent years, the U.S. federal government has assumed more responsibility for law enforcement, criminal justice remains primarily a state- and local-level operation (Richman, 2000). Within this institutional environment, criminal justice agencies tend to be highly aware of jurisdictional boundaries and extremely protective of organizational information assets (Gil-Garcia *et al*, 2004), suggesting that criminal justice agencies should be particularly aware of their identities.

Policymakers and managers are actively attempting to address the technological challenges that have resulted from the criminal justice system's institutional complexity by developing IJIS, primarily to facilitate coordination and the sharing of information. In addition to the

underlying technology, an IJIS has its own management structures, governance mechanisms, and technological assets. Though IJIS can serve public safety officials in multiple operational domains (including fire, hazardous materials, and transportation), they primarily serve law enforcement and criminal justice agencies, such as courts, probation and parole, and prisons/corrections (Williams *et al*, 2009).

Research design

Three theoretical propositions grounded in Albert & Whetten's (1985; Whetten & Mackey, 2002; Whetten, 2006) theory of organizational identity guided data collection and analysis (see Table 2).

Proposition 1 (P1) states that organizational identity is reflected in the processes through which organizations procure, design, and deploy ICT. Organizations will have processes and structures that both reflect their members' understanding of the organization's identity [*ideational*] and represent the organizational features that make the organization unique [*definitional*].

Proposition 2 (P2) states organizational identity is reflected in the material arrangements of ICT. If organizational system developers rely on organizational identity as a referent in developing new systems as posited in P1, then it follows that the material outcomes of the systems developed will reflect those referents [*phenomenological*].

Proposition 3 (P3) states that differences in organizational identity produce corresponding differences in the organizational processes related to, and the configurations of, ICT. If organizations have unique identities, and organizational ICT reflect those identities, then the unique attributes of identities should exhibit unique features and configurations of ICT [*definitional*, *phenomenological*].

To test these three theoretical propositions, this study conducted a comparative case study of two of the preeminent IJIS: the Automated Regional Justice Information System (ARJIS) and the Pennsylvania Justice Network (JNET). ARJIS has been in existence in various forms since the early 1980s and serves the greater San Diego Metro Region in California, and is widely recognized as one of the most successful IJIS initiatives and is often cited as an exemplar for other practitioners to follow (National Association of State Chief Information Officers, 2003). JNET, formally established as a Commonwealth agency in 1997, provides access to criminal justice data throughout the state of Pennsylvania. Since its inception, JNET has experienced rapid growth. Like ARJIS, JNET also has been recognized for its success as an IJIS (Commonwealth of Pennsylvania Office of Administration, 2010).

Analytic induction was the method used to test the theoretical propositions across the cases. Analytic induction is well established as an analytical method in the social sciences (Cressey, 1950; Robinson, 1951; Glaser, 1965; Yan & Gray, 1994). As an inductive process, analytic induction tests a set of theoretical propositions across cases. Where the theoretical propositions fail to explain elements of the new case, they are refined to account for data unsupported by the proposition (Robinson, 1951). As the propositions are refined with each case, they become increasingly confirmable, achieving a 'practical certainty' of their validity. In this way, analytic induction is similar to literal replication as described by Yin (Yin, 2003). With each case that confirms a proposition or hypothesis, it becomes increasingly likely that it is true for most general cases.

Data collection & analysis

Case data were collected over a period of two-and-a-half years, from 2006 to 2009. Collected data consisted of 14 (six at ARJIS, eight at JNET) semi-structured interviews, 448 primary documents, and 30 h of direct observation across both cases (see Table 3). Both ARJIS and JNET are small organizations with fewer than 10 full-time employees. Of those, only a subset could speak to both the ICT design process and the IJIS identity. In addition, given the small size of the organizations, data saturation was reached with relatively few interviews; as a result, conducting additional interviews would provide little additional insight. All interview data were recorded digitally and then transcribed.

Table 3 Data collection itemization

Source	*ARJIS*	*JNET*
Interviews	Total: 6 Interviews Key Informant (1) Project Manager (3) Lead Programmer (2)	Total: 8 interviews Key informant (2) Communications Director (2) Architectural Manager (3) Design Manager (1)
Documents	281	167
Direct observation	None	30+

Table 2 Theoretical propositions

	Proposition	*Theoretical construct*
P1	Organizational identity is reflected in the processes through which organizations procure, design, and deploy ICT.	Ideational, definitional, phenomenological
P2	The material arrangements of organizational ICT reflect organizational identity commitments.	Phenomenological
P3	Differences in organizational identity produce corresponding differences in the organizational processes related to, and the configurations of, organizational ICT.	Definitional, phenomenological

In both cases, data collection began with an interview of a key informant. An organizational member is considered a key informant when he or she is considered knowledgeable about the subject of the interview and willing to communicate his other knowledge (Tremblay, 1957; Kumar *et al*, 1993). The key informant in both cases was the IJIS chief executive. With the exception of the JNET design manager and the key informants, all subjects were interviewed a minimum of two times for one hour. Initial interviews employed a derivative of Bartel's (2001) method for eliciting perceived organizational identity in which the informant is asked to assess their perception of the organization's identity (the ideational component of identity); what distinguished their organization from other similar organizations (the definitional component of organizational identity); and to provide general understanding of the IJIS organizational practices and technological systems. The informant was asked questions such as 'Who is ARJIS?' and 'How is JNET different from other IJIS?'

Coding of interview data occurred in two phases, using qualitative coding and analysis software (*nVivo*). The first phase consisted of coding using four *a priori* codes (described in Table 4). These codes represented constructs of interest (organizational features, organizational technologies, and organizational governance processes, such as rulemaking, budgeting and dispute resolution, and theoretical constructs (the three dimensions of organizational identity). Subject responses were coded as 'identity' if they spoke to perceptions or defining characteristics of the organization. The three other *a priori* codes, derived from the research questions, provided the basis for further sorting of subject comments into general topical categories. The second phase consisted of coding identity claim statements as identity attributes using the language of the subjects themselves. This process produced a set of identity attributes for both organizations. For example, an identity statement was coded as (*Commonwealth, Information Broker*) if a subject commented, 'We are the Commonwealth's criminal justice information broker'. This process produced a set of identity claims that were common across subjects.

A second round of interview was conducted upon completion of the first-round data analysis, and was used to member-check the initial findings. The author presented interview subjects with organizational identity statements derived from the initial analysis and asked the subjects to assess the degree to which they felt the statement was an accurate reflection of the IJIS identity. When subjects identified an identity statement as accurate, they were then asked if they were able to provide a specific example of how that statement was reflected in the IJIS practices and technologies (the phenomenological component of organizational identity).

Primary documents and direct observations were a significant source data used to supplement the interview data. In total, 281 primary documents (4,284 pages) were coded and analyzed in the ARJIS case, and another 167 primary documents (4,285 pages) were coded and analyzed in the JNET case. These documents included meeting minutes, network diagrams, system models, governance agreements, applicable regulations, legislative directives, and public and private presentations. Meeting minutes in particular were useful to this analysis as they documented how system design decisions were made at a strategic level. Direct observation consisted of observing officers in the field, attending staff, management, and user meetings and taking detailed notes of what was observed. Officers in the field were observed to get a sense of how the system was used in practice. Meeting observations served to inform the document analysis and to observe first organizational design processes and negotiations. Documentary and observational data were initially coded using the *a priori* code set and then, as with the interviews, identity claims were coded using informant language.

Once coded, thematic conceptual matrices were used to organize the data. Thematic conceptual matrices are techniques used to order data conceptually (Miles & Huberman, 1994). The codes *technology*, *organization,* and *governance* represented dimensions of the IJIS, and were used as column headings. Identity claims were then clustered by similarity to provide the themes that comprised the row headings. Finally, the data were entered into the matrix based upon how it had been coded (as described previously), and then compared for similarities and differences for drawing conclusions.

Findings

Analysis of the case study data revealed that ARJIS and JNET exhibited unique, multi-faceted organizational identities. The differences in the identities of ARJIS and JNET reflected

Table 4 A priori codes

Code (a priori)	*Description*
Organization (OR)	Describes organizational details, features, structures, system development practices, and processes.
Technology (IT)	Describes specific organizational technologies, features, and functionalities.
Governance (GV)	Describes governance or decision-making structures, processes, or examples.
Identity (ID)	Describes an organizational identity commitment.
(ID: I) Ideational	Based in informant perception.
(ID: D) Definitional	Reflected in features of the organization.
(ID: P) Phenomenological	Reflected in organizational action or discourse.

differences in the governance structures and design processes of each organization [P1]; and in turn, to differences in the ways in which the technology artifacts were materially arranged [P2, P3]. ARJIS identified itself as a collaborator, providing both social and technical solutions to the region's criminal justice practitioners. JNET identified itself as an information broker for the Commonwealth of Pennsylvania, providing access to back-end criminal justice data stores to its partner agencies. Tables 4 and 5 summarize the organizational identities of ARJIS and JNET, respectively.

ARJIS

The ARJIS identity is best described as a collaboratory – a network form of organization built around shared ICT and processes, modes of communication, norms, and shared values (Cogburn, 2001). Within this broader definition, the ARJIS organizational identity exhibits three facets (see Table 5). The ARJIS organization sees itself as the centre for regional collaboration on regional public safety problems; as the primary service and technology provider for regional criminal justice agencies; and as a support system for law enforcement and public safety officials operating in the field.

A centre for regional collaboration ARJIS management and staff view ARJIS as a centre for regional collaboration. Collaboration among partners is central to the organization's self-perception, and it serves as a key dimension upon which management measures organizational success. The membership sees this emphasis on collaboration as key distinguishing feature from other IJIS and criminal justice agencies. In practice, ARJIS management strives to maintain the standing of the organization as the locus of regional criminal justice collaboration, and getting member agencies to collaborate through ARJIS is a highly prized outcome that validates their organizational existence. As the Project Manager noted:

> ARJIS fosters participation [and] cooperation. We foster relationships between agencies. My understanding is, compared to other regions in the country, our users cooperate more. I just love seeing a detective from National City talking to a detective from Carlsbad, where frankly, they might not ever have crossed paths if they hadn't come to some ARJIS-sponsored function.

Absent ARJIS, this type of serendipitous collaboration would be otherwise unavailable. This ability to provide a collaborative opportunity is critical to ARJIS's success as an organization. The Project Manager further articulates:

> The one reason we have been so successful is because of our governance and because of our strong executive leadership that is so collaborative. The thing that they've all agreed on is that they leave their egos and attitudes in the closet; they go into a room and they are all equal. Once again, that same equal thing, each agency is just as important [as another] no matter what it is. They continue to embrace that.

ARJIS's ability to serve as a locus for regional collaboration is a significant source of organizational pride and something the membership sees as differentiating ARJIS not just from its member organizations, but also other IJIS systems.

A provider and facilitator of public safety technology The second facet of the ARJIS organizational identity is that of a provider and facilitator of regional public safety ICT. The ARJIS vision statement describes ARJIS as the

Table 5 Facets of ARJIS' identity

Facet of identity	*Description*	*Example*
Centre for regional collaboration	ARJIS management sees the organization as the centre of regional collaboration among criminal justice partners. The organization exists to facilitate that collaboration.	Negotiation of data entities, definitions, and attributes among representatives from participating agencies to ensure standardization.
Provider and facilitator of regional criminal justice ICT	ARJIS management sees the organization as both providing and facilitating the development and implementation of ICT within the region. To be successful, ARJIS management believes the organization must be capable of providing technological solutions and facilitating their development in the member agencies themselves.	ARJIS negotiated the contract with Verizon on behalf of member agencies to provide wireless access to the ARJIS system.
Criminal justice tool	The management team believes that 'serving cops' as the organization's reason for being. Organizational discourse and activity is fundamentally oriented around this motivation.	Designed Global Query application to provide accurate, detailed information quickly to cops in the field.

'convening agency for regional information technology'. The Senior Programmer states this identity more explicitly:

> ARJIS is a clearinghouse for data; law enforcement data in the San Diego region. We take in virtually every piece of paper that an officer touches or creates and we pull it into a central database that other agencies can then turn around and access, so that if a car is involved in a bank robbery in one place, that officer that stopped a car in another place will find out that it matches the suspect's description. That, in a nutshell, is what ARJIS does.

Examples of the organization functioning in this role include its acting as the collective representative of the member agencies in the negotiation of contracts for mobile data service; the procurement of hardware, such as handheld devices; and the petitioning for grant funding from state, federal, and private-sector organizations. Having ARJIS negotiate a contract for mobile access on behalf of its members provides the member agencies with greater bargaining power because they are negotiating collectively and it prevents a dynamic where individual member agencies are competing against each other for shared services.

Even though the ARJIS organization strives to be the central location for criminal justice ICT within the region, other agencies have continued to pursue their own ICT procurement and development. ARJIS cannot prevent, and it is not in ARJIS's interest to prevent, individual agencies from pursuing their own ICT agendas. An attempt by ARJIS management to impose its will on other agencies regarding technology would run counter to its collaborative identity, and result in resentment and resistance from its member organizations. Thus, ARJIS identifies itself as both a provider and facilitator of regional criminal justice ICT: management understands that different member agencies have different, and often competing, technology needs and resources. Larger member agencies have extensive ICT infrastructures and budgets, while smaller member agencies may be limited to a few desktop workstations. Attempting to replace the highly entrenched infrastructures of the larger agencies would be a futile endeavor and so ARJIS management seeks to facilitate member agencies' existing systems with complementary technologies and applications, such as mobile wireless access. Simultaneously, ARJIS acts as a technology provider for smaller agencies otherwise incapable of sustaining a large ICT infrastructure for fiscal or political reasons.

A criminal justice tool for police officers The third facet of the ARJIS organizational identity is as a tool to aid police officers working in the field. Management places significant value on the development of ICT and applications that have a direct impact on public safety operations and a high degree of utility for the patrol officer, investigator, and data analyst engaged in routine criminal justice activity. 'What is in it for the user?' is the dominant refrain in system development discussions. The Senior Programmer stated:

> We have a lot of projects going on, and as you see, we are not a very big place. And, so I guess really, my first question is, do my users want this? I mean, is this useful? Is it appropriate? Is it relevant? Is somebody already doing this smarter than we are?
>
> I think the ARJIS system is different because it is so, based on user requirements and a business case established up front. The users are involved in the annual work plan of ARJIS and the development of any and all applications from beginning all the way through to the end.

The Project Manager echoed this sentiment:

> The technology is secondary to the functionality, but I mean we're pushing some functional issues that, more common to business, law enforcement has not necessarily caught up with. So we're trying to bring in that functionality for our users, so that tends to be what pushes our technology more than anything else.

Providing functionality to the user trumps fulfilling the needs of any single member agency at ARJIS. Utility to the officer in the field is the dominant design criterion. The ARJIS chief executive, herself a former police officer, knows from personal experience that new technologies or features will go unused when perceived as trivial, awkward, or useless by the users in the field. Further, she understands the tangible risks that an ineffective, or difficult-to-use, system poses for both the officer working the beat and the public. As chief executive, she has communicated to and instilled that knowledge in her entire management team. The management team, in turn, communicates this commitment to its regional partners, technology providers, and users; they reference it in making design decisions, and emphasize it in describing ARJIS to outsiders.

JNET

JNET's organizational identity is that of a Commonwealth (state government) agency that brokers information among Commonwealth partners and criminal justice agencies. The state-level orientation of JNET is very strong and drives organizational decision-making (Table 6).

Unlike ARJIS management, who perceive their organization as the central provider of public safety ICT and information, JNET management sees their organization as a facilitator of access to information.

A commonwealth agency JNET management perceives the identity of the organization to be, foremost, an agency that serves the Commonwealth government. The needs and interests of state government agencies are central to JNET's organizational and technological agenda. The chief executive repeatedly emphasized the organization's focus on meeting the needs of state

Table 6 Facets of JNET's Identity

Element of identity	*Description*	*Example*
Commonwealth agency	JNET management team views the organization as primarily a provider of services and technology to Commonwealth government customers.	When prioritizing potential projects, Commonwealth agency projects receive greater weight than municipal agency projects.
Information broker	JNET management repeatedly stresses that the organization is a broker of information to partnering agencies.	JNET connects to each system individually and has minimal federation of queries or results.

agencies in decision-making and system-development processes. Other members of the JNET senior management team echoed this focus: JNET's Application and Development Manager emphasized how JNET strives to be a service provider to state agencies:

> I hope that JNET becomes a service provider of web services to other agencies within the public safety arena. We have the web services right now, [but] the other agencies aren't ready to consume them. Once they catch up, I think that could become a major benefit to the Commonwealth.

State agencies are JNET's primary clients and beneficiaries. Management references this facet of JNET's identity in both its internal and external communications. When presenting JNET to outsiders, the management team describes JNET as 'the Commonwealth's information broker', and 'the collaborative effort of 16 state agencies.'

JNET's position within the structure of the Commonwealth government has only become more central to its identity as the organization has grown and matured. JNET's Architectural Manager commented:

> When [I say] operationalizing JNET, [I mean] more of getting into a stable platform, where our level of maturity within the Commonwealth government is more attached [as an organisation]. Because again, when we first started we were actually working for the state police, now we're Office of Administration.

The interviewee is describing the transition of JNET from what was simply a project of the Pennsylvania State Police to a full-fledged state agency. When the Office of Administration incorporated JNET, JNET cachet increased within the broader government. Also, attaining independence as an agency further served to strengthen JNET's identity as a provider to Commonwealth agencies rather than simply the state police.

An information broker The second facet of JNET's organizational identity is that of public safety information broker. Whereas ARJIS's identity was that of a central source of public safety information, JNET identified itself as a provider of access. The management mantra is 'access not ownership'. Statements from three different members of JNET's management team demonstrate how powerfully 'brokerage not ownership' has taken hold as a facet of the organization's identity. JNET's Chief Executive stated:

> When I look at JNET versus any other private or public sector [agencies] out there that are claiming to be integrators of public justice data, I see two major differences. First, we don't store, retain, or maintain data, and I think a lot of other agencies are collectors and providers of data. The other difference is that we are developers of systems that need to be – that are used to broker that information.

When asked how they would describe JNET to someone who was unfamiliar with the organization, both the JNET Architectural Manager and the JNET Project Manager invoke the broker identity:

> I would say JNET is the broker for multiple data sources within the justice community in order to increase public safety and sharing that information. JNET Architectural Manager

> JNET, I think, is as we're pretty much supposed to be: we're the facilitator of all the other agencies that provide data. We're the facilitating organisation that should know what's going on and be able to keep everything rolling and spinning. JNET Project Manager

JNET identifies so strongly as a brokerage organization in part because of the institutional barriers it had to overcome early on in its existence. Management had to overcome the reticence by agencies to relinquish any control over their data. Wresting control over the data from contributing agencies was unfeasible; thus, JNET leadership chose to obtain access and provide the interfaces to the systems of the other agencies. Providing connectivity and application development services for individual agency systems was a much more tractable problem than attempting to get those same agencies to relinquish control of their data. As will be shown below, this identity commitment has important consequences for the design of JNET's technological infrastructure.

The impact of identity on organizational features and technologies

How have the differences in the identities of ARJIS and JNET been manifested in the organizational practices of the two organizations and in their ICT. Data analysis

revealed that, though both ARJIS and JNET have similar organizational missions (facilitating information sharing), differences in their organizational identities align with differences in their design and governance processes (P1); and subsequently, differences in the systems that have resulted (P2, P3).

Organizational identity shapes ICT design and governance (P1) The governance processes and structures of both ARJIS and JNET reflect their unique organizational identities. The ARJIS governance mechanism – a Joint Powers Agreement (JPA) – and its committee-based approach to system development consistent with its identity as a collaboratory. JNET's identity as a Commonwealth agency reflects the composition of its governance committee and its process for determining which ICT project to take on or prioritize.

Regional collaboration vs serving the Commonwealth Fundamental to ARJIS's collaborative identity is its governance mechanism: a JPA. This is the legal agreement that instantiates ARJIS as an organization and sets the rules by which member agencies participate. The agreement specifies how member agencies are assessed fees to finance ARJIS: larger agencies pay more; smaller agencies pay less. Decision-making power is distributed equally among member agencies regardless of size or contribution to the ARJIS operating budget. The one agency-one vote dynamic governing ARJIS is critical to ARJIS's success as a collaborative organization because it prevents the largest agencies from dominating the discourse and governance of ARJIS. This voting model permeates all levels of the ARJIS governance hierarchy and plays a key role in facilitating collaboration among ARJIS and its partners. The ARJIS Chief Executive commented:

> I consider ARJIS [to be] very democratic, you know, our one agency-one vote model. For instance, at our chiefs' level, I think that helps balance the playing field between the large agencies and the small agencies.

ARJIS approaches the design of its ICT as a collective process through which member agencies attempt to negotiate their individual needs into the final design. All the member agencies have representation on the committees and working groups that comprise the ARJIS governance structure. Through these committees, individual member agencies can propose requests for functionality, access, or other requirements for the system. Chiefs of the various member agencies often propose new functionality or modifications to the existing technological architecture. Committee members then negotiate the proposal; and, if ratified, delegate proposed system change to the ARJIS working groups for action. The ARJIS Security Centre (a suite of authentication and encryption applications) provides an illustrative example of this process in action. The Project Manager explained the system:

> We have a new authentication system. This is where all of our users, usernames and passwords are kept. We call it the ARJIS Security Centre and each agency has an administrator that has been trained to go in and reset a password or create new users or delete this cop who retired. So, one of the things the chiefs asked for was could the users be warned before their passwords expire, and not let them expire and then notify them? So, we went to our programmers and they implemented a feature from the Security Centre that has an e-mail component.
>
> Then, we crafted up a little e-mail and, what happens now, is we watch their passwords and send them a courtesy e-mail that notifies them their password will expire in 15 days. It provides them a link to change their password. If they ignore that e-mail, they get another in 7 days with a link. And finally, they get one that notifies them their password has expired and provides another link. They have never had such proactive alerting on their passwords before. That [suggestion] came from a chief, and we turned it around and put it into production.

More often, a member agency may make a request at either the Business or Technical working groups where, if approved, it is sent to the other committee for approval. Upon approval by both committees, the proposed design change works its way up through the Management Committee and the Public Safety Committee for final approval. In either case, the design process is highly collaborative at all levels of the process resulting in a design outcome that reflects an amalgamation of the various member agencies' design requirements.

Consider, for example, the system data dictionary. Addition of new data codes to the ARJIS database to account for new types of crime, changes in criminal law, and to meet agency needs is continuous. Proposals for new codes are made in committee where, through negotiation, the final form of the code is defined. These new data codes are then incorporated into the ARJIS database and all the member agency systems to ensure conformity. Because the member agencies collaborate on design of the data standards, there is an additional peer pressure among the member agencies to ensure compliance with the data standards and code definitions. When an individual agency fails to comply, their representatives often receive kindly intended, but undesired, derision from their peers. This social interaction among the member agency representatives serves as an informal mechanism for ensuring compliance with collaborative design and is so effective that the formal mechanisms for ensuring compliance are rarely used.

As seen with ARJIS, JNET's governance processes and structures reify its identity as a Commonwealth agency. The JNET organization resides within the larger government bureaucracy, and JNET management reports directly to the Office of Administration, a cabinet-level office in the

executive branch of the Commonwealth government. The voting membership of the committee charged with overseeing JNET is comprised exclusively of representatives of Commonwealth government agencies. All of these factors serve to reinforce JNET's identity as a Commonwealth organization in the service of other Commonwealth agencies (Figure 1).

JNET management is required to report to its Steering Committee. JNET, though, has reached a level of organizational maturity that enables its management team to conduct daily operations autonomously, without the direct involvement of its governing committees. The Steering Committee now primarily performs an oversight function, and occasionally, the Executive Director will seek its guidance in resolving particularly difficult issues.

No local, regional, or federal agencies have participatory power in the Steering Committee (two representatives from local agencies participate, but with no voting power). Steering Committee meeting minutes reveal that the agenda of the committee almost exclusively deals with Commonwealth government issues and priorities. For example, in 2007 the only mention of counties noted in the meeting minutes was in the form of status updates related to on-going JNET projects, for example, 'We've deployed to five more counties this month'. Non-Commonwealth agencies are, in practice, limited to consuming JNET technologies with minimal influence on the governance of the JNET system.

Similarly, JNET's strategic and operational planning processes reflect JNET's identification as a Commonwealth agency. The management team uses the larger government's strategic plan, known as the Keystone Plan, as the basis for its own strategic planning. Projects that do not align with the Keystone Plan are not implemented because they have no organizational value for JNET's management team:

> The Keystone Plan was published, and then we developed a five-year strategic plan. Once that plan was completed, we had to go through and make sure everything we wanted to do as an agency aligned with the Keystone Plan. Then, we developed a business plan that has to align with the strategic plan. Each year, every project has to tie back to the strategic plan and the Keystone Plan. If we can't [tie the project back to those plans], there's no value in completing that project. JNET Chief Executive

Operational planning at JNET also reflects its identification as a Commonwealth agency. The JNET management team prioritizes which projects to take on and where to assign resources through use of a scoring matrix. Projects are scored on dimensions such as: what agency the project is for, who is funding the project, the ability to deliver quickly, etc., with Commonwealth agency projects that produce cost savings for the Commonwealth government more broadly receiving precedence in JNET's project selection process. With this weighting scheme in place, JNET dedicates its resources almost exclusively to Commonwealth-related technology projects. If there is no direct, identifiable, benefit to a state government agency a project is not selected, though it may ultimately serve more users. As JNET's Chief Executive commented:

> Part of that vetting process for a project is, 'Who is going to benefit from it?' I'll be honest, if a local cop's going to benefit from it and the state police have no interest, it may not occur. Local, county, and municipal government is as essential to me [and JNET] as our state government. The difference is they don't sit on our governing committee.

Although non-Commonwealth organizations may use JNET heavily and reside in the same operational domain (public safety/criminal justice), they have little to no influence over JNET's development trajectory.

To summarize, the organizational identities of ARJIS and JNET influence their respective system development processes. ARJIS's identity as a collaboratory is instantiated in governance structures and development processes that facilitate collaborative system development and member agency buy-in. JNET's identity as a Commonwealth agency is reflected in its system development process where Commonwealth-related projects are prioritized; even though JNET's user constituency spans local, county, state, and federal levels of government.

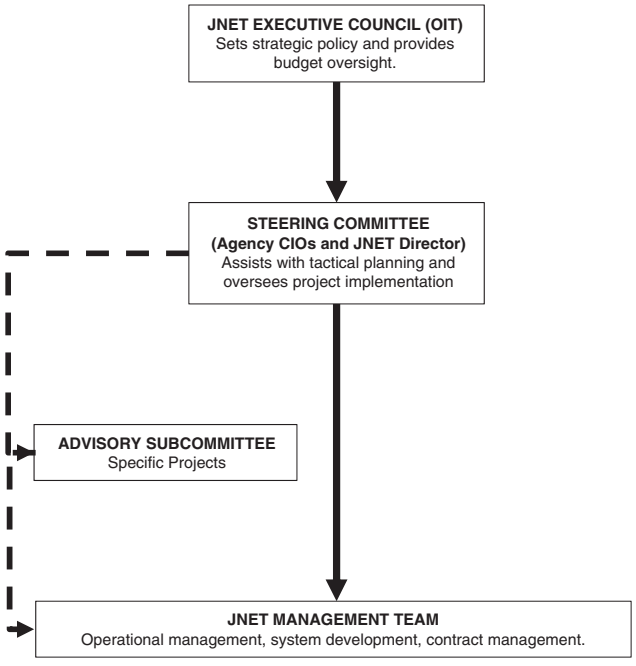

Figure 1 JNET management structure.

Organizational identity commitments shape design outcomes (P2, P3)

Though ARJIS and JNET both exist to facilitate the sharing of criminal justice information, their ICT differ in two

significant ways. First, ARJIS collects, standardizes, and stores its member agency data, while JNET does not collect or store any data. Second, ARJIS provides access to multiple data stores including its legacy mainframe through a single, federated query application, while the JNET design is that of a portal, providing point-to-point connections to individual systems. These two differences in design reflect the identity differences of ARJIS and JNET.

Centralized versus distributed ARJIS has developed their suite of information technologies in a manner consistent with their identity as a central provider for criminal justice information and as a tool for officers in the field. As the central provider for criminal justice information and technology, ARJIS is the central point of access to local member-agency data for both member and non-member agencies, such as the United States Federal Bureau of Investigation. Local data are aggregated, standardized, and stored in the legacy mainframe system and is accessible through a web interface designed by the ARJIS organization. The system also provides centralized access to external systems such as the California Department of Motor Vehicles driver's license database (Cal-Photo), the state of California's database of registered street gang members (Cal-Gang), and the state of California's law enforcement records database (CLETS). Finally, ARJIS is also the provider of the hardware, software, and connectivity (contracted through a private vendor) for mobile access to these systems. In sum, ARJIS is the 'place to go' for the region's criminal justice community for access to local, state, and federal criminal justice.

Conversely, as an information broker, JNET neither hosts nor standardizes the data to which it provides access. Rather, JNET mainly provides the connectivity to a combination of 25 applications and database systems. The database systems that JNET connects to are almost exclusively Commonwealth agency systems, such as the state courts system (APOC), the Department of Health's birth records database, the Pennsylvania State Police's records management system (CLEAN), and the Department of Transportation driver's license photo database. JNET has added each of its data resources individually and separately from other data resources over time. Rather than standardizing the data across the individual system, as ARJIS has done, JNET uses middleware to provide compatibility between the data store and the JNET portal. The result of this approach is a system architecture that operates similar to a turntable in a locomotive roundhouse: users (locomotives) enter the JNET portal (the roundhouse) and portal redirects the users to the individual systems (spokes) they need to access. This approach to design has had important consequences for the ways JNET users get access to information.

Federated versus point-to-point The ARJIS system reflects its identity as a tool for police officers in multiple ways. In addition to providing access to all of the local criminal justice data housed in the ARJIS mainframe, ARJIS has developed a simple-to-use application that allows users to perform federated searches of multiple databases. This application is called Global Query. The design rationale for making Global Query a federated query tool was to maximize the simplicity of use for the officers in the field.

> [But] the whole goal for the system was to keep it simple. Make it easy for the cops; give them a quick hit with valuable returns. Don't make the query or the returns too complicated. I think it was just user-simplicity. ARJIS Project Manager

Global Query 2 provides access to local booking photos and arrest warrants, CLETS, Department of Motor Vehicle (DMV) records, and officer notifications through a single interface. The Global Query 2 application allows users to query all these systems with the submission of a single query. As a result, users only have to remember a single set of credentials; the number of pages a user has to navigate was reduced from 36 to 2; and results are returned in a single, consistent format, making them easier to comprehend. The design of Global Query 2 is oriented towards making the application quick and easy to use by criminal justice practitioners, who are largely non-technical in nature and are often using technology in a setting where sustained focus on using it could be potentially dangerous; and for whom access to information is mission-critical. For the ARJIS organization, designing Global Query 2 to be simple and efficient to use was a necessity. For the JNET organization, where providing access was the overriding identity concern, a very different design outcome resulted.

JNET's identity as an information broker has meant that the JNET organization has not collected, standardized, or stored information. Indeed, JNET's primary design focus has been twofold: to provide connectivity and to develop an application for accessing the connected systems. Over time, JNET established connectivity to individual systems independent of any other systems to which the system connects. In practical terms, JNET designers added new systems to the JNET portal, but did not integrate with the existing systems.

This approach of incremental addition of connected systems had important consequences for JNET's portal application used by practitioners in the field. Unlike ARJIS, with its federated search, JNET requires its users to navigate to the specific systems they would like to search. For example, a patrol officer who detains a motorist for exceeding the posted speed limit must follow a complex process to obtain all of the salient information they need. First, the officer access one system to verify the driver's record. Then the officer must return to the portal to access a second system to determine if the driver has any outstanding wants or warrants. Finally, the officer must once again return to the portal to access a third system and determine if the driver has a criminal record. This usage pattern reflects a design approach to the problem of accessing multiple databases that is much less elegant and efficient than ARJIS's federated query. The approach,

however, is consistent with the JNET organization's identity of brokering information and serving Commonwealth agencies as opposed to collecting information and serving police. While JNET has attempted to improve usability through the introduction of a single federated query of a single agency's system, their ability to implement a federated query on a larger scale, like Global Query 2, remains elusive because of incremental approach to adding systems that they have taken previously.

Discussion

The research presented here adds to our understanding of the impact of social and organizational factors on IS development in three ways. First, as the cases make clear, organizational identity mediates the processes through which organizations develop, procure, and deploy ICT through both the members' understandings of the organizational membership and the explicitly codified identity commitments, such as vision statements and governance agreements. The managers and system developers in organizations deliberately seek opportunities that align with, while eschewing those that violate, a sense of their identity. The influence of organizational identity on the development of organizational ICT suggests that both practitioners and scholars of organizational IS would benefit from developing greater knowledge of organizational identity dynamics.

Second, the specific material configurations and features of an organization's ICT reflect the mediating influence of organizational identity on the organization's system development processes. Just as ARJIS's and JNET's systems reflect their organizational identities, other organizations are likely to find that specific features and configurations in their own IS reflect their identity commitments.

Third, since the material features of organizational ICT trace back to an organization's identity, the ICT of organizations with different identities should exhibit different features and configurations even when intended for the same general purpose (Whetten, 2006). Indeed, the cases presented have shown that this variation is precisely what occurs. Both ARJIS and JNET are organizational and technological ensembles created for the express purpose of integrating heterogeneous criminal justice information. Yet, though they both make use of many of the same technologies (e.g., wireless access), the manner in which each implements those technologies is idiosyncratic in ways that align with their organizational identity.

Organizational identity is both a facilitator and barrier to ICT implementation

An implication of this research is that organizational identity both enables and constrains IS development within organizations. IS represent phenomenological instantiations of the organization's identity commitments. Existing systems, particularly large systems, play an active role in shaping the development of new systems (Chae & Poole, 2005). Organizations who attempt to implement or develop IS that diverge radically from their identity commitments are likely to find the process exceedingly difficult, and perhaps ultimately destructive (Ravasi & Schultz, 2006).

Conversely, organizational members are likely to gravitate towards those ICT that serve to reinforce positive aspects of the organization's identity, rather than those that threaten the established identity (Elsbach & Kramer, 1996). In this way, the role of organizational identity in shaping an organization's IS is similar to that found in firms who develop ICT for the market by filtering the membership's perceptions of the ICT options available to the organization (c.f., Tripsas, 2009). In this way, organizational identity may be a form of domain knowledge or shared understanding that can bring about strategic alignment of ICT (Mosse & Byrne, 2005; Preston & Karahanna, 2009). Managers involved in systems development would benefit from developing an explicit understanding of their organization's identity. One possible means of achieving this understanding may be through conducting an 'identity audit' – similar to Burns 'cultural audit' (Chan & Reich, 2007) – that reviews alignment of organizational identity with both organizational and IT strategy prior to embarking on development.

A second implication of this research is that the degree to which the identities of the integrating organizations align will determine the extent to which integration of IS across organizational boundaries will be successful. We can infer from the prior implication that organizations whose identities closely align would seem more likely candidates for deeper integration because their technologies will be more closely aligned, a dynamic similar to what institutional theorists refer to as *mimetic isomorphism* (Scott, 2001; Hossam, 2005). Conversely, organizations whose identities are divergent are likely to be limited in the extent to which they can integrate their systems. For example, providing access would be the limit to which ARJIS and JNET could integrate because of their divergent identities. This may also explain why, to date, IJIS initiatives have been primarily localized efforts, focusing on a single level or branch of government or a specific community, as identity isomorphism would appear to be more likely among organizations in closer institutional or geographical proximity. This research did not explore the interplay between the identities of the individual member agencies within ARJIS and JNET, so this implication remains a tentative pending additional research.

Another implication of this research for organizational identity theory is that the instantiation of an organization's identity in its IS may make the organization's identity much more resistant to significant change (Ravasi & Canato, 2010). Few organizations successfully manage core change (Barnett & Carroll, 1995) or radical transformation of their IT infrastructure (Hill & Rothaermel, 2003). Considering the extent to which the identities of ARJIS and JNET permeate their respective organizational structures, processes, and technologies, significant alteration of their identities would require corresponding alterations

to those same structures, processes, and technologies. The theoretical argument made here is not that organizational identity is a permanently fixed feature of the organization, but rather, absent a significant catalyst (e.g., Dutton & Dukerich, 1991), organizational identity changes at the periphery while maintaining its central features. Indeed, it is difficult to imagine an instance where an organization could undergo radical identity transformation without the destruction of the prior identity. To the extent that the central features of an organization's identity change, they do so slowly over time. Thus, a strategy of incremental technological change combined with incremental – or evolutionary (c.f., Besson & Rowe, 2012) – organizational change management may be the more useful approach to development of new IS that diverge significantly from the extant organizational identity (Markus, 2004).

Contributions

This paper makes two contributions. First, this paper contributes to IS research in drawing attention to the important role organizational identity plays in how organizations develop their IS. This paper provides further support for Orlikowski & Barley's (2001) argument that organizational theory is an important resource for understanding organizations and their technologies. Organizational identity has received widespread attention in the management literature (c.f., Ravasi & Van Rekom, 2003; Corley *et al*, 2006; Whetten, 2006) suggesting that it is salient to the IS community. Yet the influence organizational identity on IS, to date, is largely unexplored in the IS literature (Kjaergaard & Gal, 2009). This paper has shown that organizations rely on organizational identity in deciding both their approach to system development and the material features of the technology. In doing so, this paper serves as an important first step towards understanding the relationship between organizations' identities and their technologies, and provides the basis for future research into this important organizational dynamic.

Second, in providing empirical evidence of the influence of organizational identity on the material features of IS, this research informs professional practice by drawing attention to a previously unconsidered issue. There is a significant body of prescriptive literature on IJIS development within the criminal justice community. Oft-recommended practices such as getting top-management support, obtaining customer buy-in, and developing a clear business-case are common to this body of literature (Gil-Garcia *et al*, 2004; National Association of State Chief Information Officers, 2003). The research presented here suggests that IJIS managers would also be wise to understand the influence of their organization's identity on the IS they build. Absent significant internal or external pressure, attempting to adopt technologies seen as incompatible with the organization's identity are likely to meet significant institutional resistance. Organizations seeking to implement transformative technologies are likely to have more success with a strategy of incremental change that, over time, evolves the organizational identity along with the technology.

Policymakers with visions of one-size-fits-all, wholly integrated, criminal justice information systems – particularly in the United States where local control is the dominant operational mode – ignore organizational identity at their peril. Attempts to homogenize criminal justice technology on a large scale with disregard for organizational identity are likely to be unsuccessful. This paper suggests that the wiser approach is to seek opportunities to integrate technologies where the identities of organizations are similar or overlap, thus increasing the likelihood of buy-in from the participant organizations.

Limitations and future research

There are three limitations to the findings and implications of this research. First, the generalizability of this research is limited because, in both case studies, IS development is fundamental to the very existence of both organizations. While organizational identity clearly shaped their system development activities and outcomes, the extent of their organizational identity's influence in ARJIS and JNET may be exaggerated compared to other organizations for which IS development is a necessary but, non-core, organizational activity. In addition, both ARJIS and JNET are government organizations and, therefore, may not exhibit the same dynamics as for-profit organizations. Finally, as relatively small organizations, ARJIS and JNET may have organizational identities that are more readily perceived by the membership and thus more cohesive than we might find in larger organizations. Future research will need to study many more cases of both similar and dissimilar organizations, which will help to resolve these questions.

A second limitation of this research is that it did not test alternative explanations for the phenomena observed. As such, it is possible that there are better explanations for why the development processes and IS of ARJIS and JNET took the form that they did. It is important to note, however, that the author does not claim that organizational identity is the singular causal factor in determining the outcome observed, but rather one of many important factors, including institutional pressures, strategic alignment, financial pressures, and the presence/absence of legacy systems. One goal of future research is to attempt to measure the influence of organizational identity on systems development in relation to other factors. The reader will have to decide the extent to which this limitation affects the findings.

A third limitation of this research is the case studies presented here represent a limited timeframe in the organizational life of ARJIS and JNET. A longitudinal study would have been much more conducive to observing any changes in organizational identity within ARJIS and JNET and any resultant changes in the characteristics of the systems they,

respectively, developed. A longitudinal study simply was not feasible for the author given the available resources at the time. Longitudinal studies should be a part of any future research agenda in this area.

About the author

Michael Tyworth is an Instructor of Supply Chain & Information Systems and Management & Organizations in the Smeal College of Business at Penn State University Park. He holds a B.A. of Psychology from Penn State, a Masters of Information Science from Indiana University, and a Ph.D. in Information Sciences & Technology from Penn State. His research interests include social and organizational informatics, computer-mediated communication, and e-government. His work has been published in *Information Polity*, *The Information Society,* and several peer-reviewed conferences.

References

ALBERT S and WHETTEN DA (1985) Organizational identity. In *Research in Organizational Behavior* (CUMMINGS LL and STAW BM, Eds), pp 263–295, JAI Press, Greenwich, CT.

ASH JS, BERG M and COIERA E (2004) Some unintended consequences of information technology in health care: the nature of patient care information system-related errors. *Journal of the American Medical Informatics Association* **11**(**2**), 104–112.

BALDWIN RG (1998) Technology's impact on faculty life and work. *New Directions for Teaching and Learning* **1998**(**76**), 7–21.

BARNETT WP and CARROLL GR (1995) Modeling internal organizational change. *Annual Review of Sociology* **21**, 217–236.

BARTEL CA (2001) Social comparisons in boundary-spanning work: effects of community outreach on members' organizational identity and identification. *Administrative Science Quarterly* **46**(**3**), 379–413.

BESSON P and ROWE F (2012) Strategizing information systems-enabled organizational transformation: a transdisciplinary review and new directions. *The Journal of Strategic Information Systems* **21**(**2**), 103–124.

BRUNNINGE O (2005) Organisational self-understanding and the strategy process: Strategy dynamics in Scania and Handelsbanken. PhD thesis, Jonkoping University.

CHAE B and POOLE MS (2005) The surface of emergence in systems development: agency, institutions, and large-scale information systems. *European Journal of Information Systems* **14**(**1**), 19–19.

CHAN YE and REICH BH (2007) IT alignment: what have we learned? *Journal of Information Technology* **22**(**4**), 297–315.

COGBURN DL (2001) Globally-distributed collaborative learning and human capacity development in the knowledge economy. Globalization and lifelong education: critical perspectives. [WWW document] http://www.communitytechnology.org/products/Cogburn-LEAChapter-Revised.pdf (accessed 3 January 2009).

COMMONWEALTH OF PENNSYLVANIA OFFICE OF ADMINISTRATION. (2010) Office Of Administration: Pennsylvania Justice Network Named Finalist For Intergovernmental Solutions Award. [WWW document] http://www.thestreet.com/story/10728056/office-of-administration-pennsylvania-justice-network-named-finalist-for-intergovernmental-solutions-award.html (accessed 10 September 2012).

CORLEY KG and GIOIA DA (2004) Identity ambiguity and change in the wake of a corporate spin-off. *Administrative Science Quarterly* **49**(**2**), 173–208.

CORLEY KG, HARQUAIL CV, PRATT MG, GLYNN MA, MARLENE FC and HATCH MJ (2006) Guiding organizational identity through aged adolescence. *Journal of Management Inquiry* **15**(**2**), 85–99.

CRESSEY DR (1950) The criminal violation of financial trust. *American Sociological Review* **15**(**6**), 738–743.

DESANCTIS G and POOLE MS (1994) Capturing the complexity in advanced technology use: adaptive structuration theory. *Organization Science* **5**(**2**), 121–147.

DEWETT T and JONES G (2001) The role of information technology in the organization: a review, model, and assessment. *Journal of Management* **27**(**3**), 313.

DUKERICH JM, GOLDEN BR and SHORTELL SM (2002) Beauty is in the eye of the beholder: the impact of organizational identification, identity, and image on the cooperative behaviors of physicians. *Administrative Science Quarterly* **47**(**3**), 507–533.

DUTTON JE and DUKERICH JM (1991) Keeping an eye on the mirror: image and identity in organizational adaptation. *Academy of Management Journal* **34**(**3**), 517–554.

DUTTON JE, DUKERICH JM and HARQUAIL CV (1994) Organizational images and member identification. *Administrative Science Quarterly* **39**(**2**), 239–263.

ELSBACH KD and KRAMER RM (1996) Members' responses to organizational identity threats: encountering and countering the business week rankings. *Administrative Science Quarterly* **41**(**3**), 442–476.

FEDOROWICZ J, GOGAN JL and WILLIAMS CB (2007) A collaborative network for first responders: lessons from the CapWIN case. *Government Information Quarterly* **24**(**4**), 785–807.

FEDOROWICZ J, MARKUS ML, SAWYER S, TYWORTH M and WILLIAMS CB (2006) Design Principles for Public Safety Response Mobilization. In *Proceedings of the 7th Annual National Conference on Digital Government Research: Integrating Information Technology and Social Science Research for Effective Government* (FORTES JAB and MACINTOSH A, Eds), Association of Computing Machinery, San Diego, CA.

GAL U, LYYTINEN KJ and YOO Y (2008) The dynamics of IT boundary objects, information infrastructures, and organisational identities: the introduction of 3D modelling technologies into the architecture, engineering, and construction industry. *European Journal of Information Systems* **17**(**3**), 290–304.

GIL-GARCIA JR, SCHNEIDER CA and PARDO TA (2004) Effective strategies in justice information integration: a brief current practices review. Center for Technology in Government [WWW document] http://www.ctg.albany.edu/publications/reports/effective_strategies (accessed 3 January 2005).

GIOIA DA, SCHULTZ M and CORLEY KG (2000) Organizational identity, image, and adaptive instability. *Academy of Management. The Academy of Management Review* **25**(**1**), 63–81.

GIOIA DA and THOMAS JB (1996) Identity, image, and issue interpretation: sensemaking during strategic change in academia. *Administrative Science Quarterly* **41**(**3**), 370–403.

GLASER BG (1965) The constant comparative method of qualitative analysis. *Social Problems* **12**(**4**), 436–445.

HASLAM SA, POSTMES T and ELLEMERS N (2003) More than a metaphor: organizational identity makes organizational life possible. *British Journal of Management* **14**(**4**), 357–369.

HILL CWL and ROTHAERMEL FT (2003) The performance of incumbent firms in the face of radical technological innovation. *The Academy of Management Review* **28**(**2**), 257–274.

HOEY A (1998) Techno-cops: information technology and law enforcement. *International Journal of Law and Information Technology* **6**(**1**), 69–90.

HOSSAM A-H (2005) Institutional Theory. Theories used in IS research [WWW document] http://www.istheory.yorku.ca/institutionaltheory.htm (accessed 1 August 2007).

JONES MR and KARSTEN H (2008) Gidden's structuration theory and information systems research. *MIS Quarterly* **32**(**1**), 127–157.

KJAERGAARD A and GAL U (2009) Identity in information systems. In: *Proceedings of the 17th European Conference on Information Systems* (NEWELL S, WHITLEY E, POULOUDI N, WAREHAM J and MATHIASSEN L, Eds) pp 180–193, Verona, Italy.

KLING R, ROSENBAUM H and SAWYER S (2005) *Teaching Key Ideas of Social Informatics*. Information Today Inc., Medford, N.J.

KUMAR N, STERN LW and ANDERSON JC (1993) Conducting interorganizational research using key informants. *The Academy of Management Journal* **36**(**6**), 1633–1651.

LAMB R and KLING R (2003) Reconceptualizing users as social actors in information systems research. *MIS Quarterly* **27**(**2**), 197–235.

LEONARDI PM and BARLEY SR (2010) What's under construction here? Social action, materiality, and power in constructivist studies of technology and organizing. *The Academy of Management Annals* **4**(**1**), 1–51.

LI DA X (2011) Enterprise systems: state-of-the-art and future trends. *Industrial Informatics, IEEE Transactions on* **7**(**4**), 630–640.

LUNA-REYES LF, ZHANG J, GIL-GARCIA JR and CRESSWELL AM (2005) Information systems development as emergent socio-technical change: a practice approach. *European Journal of Information Systems* **14**(**1**), 93–105.

MANNING PK (2003) *Policing Contingencies*. University of Chicago Press, Chicago, IL.

MARKUS ML (2004) Technochange management: using IT to drive organizational change. *Journal of Information Technology* **19**(**1**), 4–20.

MARKUS ML and BENJAMIN RI (1997) The magic bullet theory in IT-enabled transformation. *Sloan Management Review* **38**(**2**), 55–68.

MERALI Y (2002) The role of boundaries in knowledge processes. *European Journal of Information Systems* **11**(**1**), 47–60.

MILES MB and HUBERMAN AM (1994) Within-case displays: explaining, predicting. In *Qualitative Data Analysis: An Expanded Sourcebook,* pp 143–171, SAGE Publications Inc., Thousand Oaks, CA.

MOSSE EL and BYRNE E (2005) The role of identity in health information systems development: a case analysis from Mozambique. *Information Technology for Development* **11**(**3**), 227–243.

NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS. (2003) Concept for Operations for Integrated Justice Information Sharing Systems. [WWW document] http://www.nascio.org/hotIssues/EA/ConOps2003.pdf (accessed 4 September 2007).

ORLIKOWSKI WJ (1993) Learning from notes: organizational issues in groupware implementation. *The Information Society* **9**(**3**), 237–250.

ORLIKOWSKI WJ (2000) Using technology and constituting structures: a practice lens for studying technology in organizations. *Organization Science* **11**(**4**), 404–428.

ORLIKOWSKI WJ and BARLEY SR (2001) Technology and institutions: what can research on information technology and research on organizations learn from each other? *MIS Quarterly* **25**(**2**), 145–165.

PRESTON DS and KARAHANNA E (2009) Antecedents of is strategic alignment: a nomological network. *Information Systems Research* **20**(**2**), 159–179.

RAVASI D and CANATO A (2010) We are what we do (and how we do it): organizational technologies and the construction of organizational identity. In *Technology and Organization: Essays in Honour of Joan Woodward (Research in the Sociology of Organizations)* (PHILLIPS N, GRIFFITHS D and SEWELL G, Eds), pp 49–78, Emerald Group Publishing Limited, Bingley, United Kingdom.

RAVASI D and SCHULTZ M (2006) Responding to organizational identity threats: exploring the role of organizational culture. *Academy of Management Journal* **49**(**3**), 433–458.

RAVASI D and VAN REKOM J (2003) Key issues in organizational identity and identification theory. *Corporate Reputation Review* **6**(**2**), 118–132.

REGER RK, GUSTAFSON LT, DEMARIE SM and MULLANE JV (1994) Reframing the organization: why implementing total quality is easier said than done. *Academy of Management. The Academy of Management Review* **19**(**3**), 565–584.

RICHMAN DC (2000) The changing boundaries between federal and local law enforcement. In *Boundary Changes in Criminal Justice Organizations – Criminal Justice 2000* (FRIEL CM, Ed), pp 81–111, National Institute of Justice, Rockville, MD.

ROBINSON WS (1951) The logical structure of analytic induction. *American Sociological Review* **16**(**6**), 812–818.

ROSE J (1998) Evaluating the contribution of structuration theory to information systems discipline. In *Proceedings of the 6th European Conference on Information Systems* (BAETS WRJ, Ed), Aix-en-Provence, France.

SAWYER S, FEDOROWICZ J, TYWORTH M, MARKUS ML and WILLIAMS CB (2007) A Taxonomy for Public Safety Networks. In *Proceedings of the 8th Annual International Digital Government Research Conference* (CUSHING JB and PARDO TA, Eds), Association for Computing Machinery, Philadelphia.

SCOTT WR (2001) *Institutions and Organizations*. Sage Publications, Thousand Oaks, Calif.

SHRIVASTAVA P and SCHNEIDER S (1984) Organizational frames of reference. *Human Relations* **37**(**10**), 795–809.

SILVA L and HIRSCHHEIM R (2007) Fighting against windmills: strategic information systems and organizational deep structures. *MIS Quarterly* **31**(**2**), 327–354.

SORENSEN C and PICA D (2005) Tales from the police: rhythms of interaction with mobile technologies. *Information and Organization* **15**(**2**), 125–149.

SPEIER C and VENKATESH V (2002) The hidden minefields in the adoption of sales force automation technologies. *The Journal of Marketing* **66**(**3**), 98–111.

TREMBLAY M-A (1957) The key informant technique: a nonethnographic application. *American Anthropologist* **59**(**4**), 688–701.

TRIPSAS M (2009) Technology, identity, and inertia through the lens of 'the digital photography company'. *Organization Science* **20**(**2**), 441–460.

UNITED STATES DEPARTMENT OF JUSTICE OFFICE OF JUSTICE PROGRAMS BUREAU OF JUSTICE STATISTICS. (2007) Law Enforcement Statistics. [WWW document] http://www.ojp.usdoj.gov/bjs/lawenf.htm (accessed 1 May 2008).

VOSS ZG, CABLE DM and VOSS GB (2006) Organizational identity and firm performance: what happens when leaders disagree about 'who we are?'. *Organization Science* **17**(**6**), 741–772.

WANG P (2010) Chasing the hottest it: effects of information technology fashion on organizations. *MIS Quarterly* **34**(**1**), 63–85.

WHETTEN DA (2006) Albert and Whetten revisited: strengthening the concept of organizational identity. *Journal of Management Inquiry* **15**(**3**), 219–234.

WHETTEN DA and MACKEY A (2002) A social actor conception of organizational identity and its implications for the study of organizational reputation. *Business and Society* **41**(**4**), 393–414.

WILLIAMS CB *et al* (2009) The formation of inter-organizational information sharing networks in public safety: cartographic insights on rational choice and institutional explanations. *Information Polity: The International Journal of Government & Democracy in the Information Age* **14**(**1**/**2**), 13–29.

WINTER SJ, SAUNDERS C and HART P (2003) Electronic window dressing: impression management with websites. *European Journal of Information Systems* **12**(**4**), 309–322.

YAN A and GRAY B (1994) Bargaining power, management control, and performance in United States – China Joint Ventures: A Comparative Case Study. *Academy of Management Journal* **37**(**6**), 1478–1517.

YIN RK (2003) *Case Study Research: Design and Methods*. Sage Publications Inc, Thousand Oaks, CA.