Growing an Organizational Field for Infrastructure: 
US State and Local Fusion Centers, 
2001-2012 
Research-in-Progress

JoAnn M. Brooks 
Syracuse University 
joannbrooks36@gmail.com

ABSTRACT

Developing information infrastructure entails changing organizations and institutions. Such changes sometimes proceed relatively smoothly, but often meet with “friction.” This paper describes the development of a national infrastructure for sharing of information among government agencies and highlights how the social, organizational and institutional changes necessary for information sharing have occurred relatively effectively. In less than ten years, the US National Network of Fusion Centers has implemented technologies and processes for sharing “threat-related” information between law enforcement and intelligence agencies across local, state and federal levels of government. Institutionally, the growth of this infrastructure has entailed developing an organizational field of state and urban area Fusion Centers. The paper describes key technological, organizational and institutional factors shaping development of this field, particularly those of institutional logics and the influence of a central agency via multiple self-reinforcing dynamics. Implications for theory, practice and research are discussed.

Keywords

Information infrastructure, institutionalization, organizational field.

INTRODUCTION

Developing information infrastructure entails changing organizations and institutions. Such changes often meet with “friction”; however they can also sometimes proceed relatively smoothly. This paper describes the development of a national infrastructure for sharing of information among government agencies, and emphasizes how the social, organizational and institutional changes necessary for information sharing have occurred relatively effectively. In less than ten years, the US “National Network of Fusion Centers” has implemented technologies and processes for sharing “threat-related” information between law enforcement and intelligence agencies across local, state and federal levels of government. Institutionally, this infrastructure growth has been accomplished through developing an organizational field of state and urban area Fusion Centers. The paper describes key technological, organizational and institutional factors shaping development of this field, especially relevant institutional logics and the influence of a central agency via multiple self-reinforcing dynamics. Implications for theory, practice and research are discussed.

RESEARCH METHODS

Data was collected from public websites – including those associated directly with Fusion Centers, those associated with Department of Homeland Security and other government agencies, public interest groups such as American Civil Liberties Union, and newspapers and other online media.

FUSION CENTERS

Fusion Centers (FCs) are now operating within almost every one of the United States. These FCs were established in response to a federal mandate to facilitate information sharing and better “connect the dots” between government agencies. According to the DHS website:
State and major urban area fusion centers (fusion centers) serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial (SLTT) and private sector partners. [http://www.dhs.gov/state-and-major-urban-area-fusion-centers – 1/13/13]

Receipt of informational inputs includes vetting for privacy concerns and entering information into databases. Analysis involves comparing new data with existing data and identifying patterns, especially “trends” across different reporting districts. Gathering involves collecting information “from various sources, including law enforcement agencies, public safety agencies, and the private sector.” (Baseline Capabilities 2008, p. 16). The “threat-related information” that is gathered, analyzed and shared encompasses a wide range of data from different levels and branches of government agencies (e.g. records of vehicle registrations, traffic accidents, mortgages and deeds, jail/prison visits), commercial service providers (e.g. financial services, ISPs, bank records, medical records and hotels), and news feeds (Fusion Center Guidelines cited in EPIC 2013). Sharing entails developing and disseminating “alerts, warnings and notifications,” and other products to audiences such as state and local police and sheriffs, other FCs, Federal Bureau of Investigation (FBI), DHS and certain private sector organizations.

Most FC employees are identified as “analysts” – i.e. they analyze the data and prepare the products; depending on a FC’s size, it could have anywhere from one to more than 50 such analysts working within it (EPIC 2013). Most FCs also have a Director that oversees operations and interfaces with other organizations. Related FC capabilities include technology adoption and use, creating and handling Suspicious Activity Reports (SARs).

FINDINGS

Emerging Organizational Field

The number of established FCs has grown since 2001. Initially there were only a few; by 2006 DHS reported 38 FCs in existence; in 2010 there were 72; and in 2011, 73 (EPIC 2013). Most FCs are based in State Police or Highway Patrol headquarters or co-located with state / local emergency management division; others are co-situated with other organizations such as state bureau of investigation or a regional agency that tracks organized crime or drug traffic (Public Intelligence 2011).

Organizational forms and capabilities of these FC organizations are at different stages of maturity and are considered to be converging (Cilluffo, Clark, Downing & Squires 2012; 2010 Baseline Capability Assessment). A small number have been identified as “model” FCs (DHS 2010b; Harwood 2013; Smith, 2011) for other FCs to emulate. The field is thus becoming more institutionalized.

Each FC becomes established within a state or local field of contention; at the same time an organizational field of FCs is emerging nationally in a broader arena of public and legal contention. As with organizational fields generally, the emergent field of FCs is embedded within and engages with other fields in the broader environment. In the FC case, these include: state, local and federal government agencies and policy organizations; public interest advocacy groups (e.g. American Civil Liberties Union); and technology developers and vendors.

“Roads to Institutionalization”

Although the number of FCs has increased and organizational forms and capabilities are converging, early FCs were relatively idiosyncratic with respect to organization and capabilities (Cilluffo, Clark, Downing & Squires 2012). Given such differences across initial organizations and uneven development of FCs over time, Colyvas and Powell’s (2006) “Roads to Institutionalization” provides a useful lens for examining the process of institutionalization. This perspective views institutionalization as a process of endogenous self-reinforcing feedback dynamics of heightened legitimacy and deeper taken-for-grantedness.

Deepening taken-for-grantedness occurs primarily at the organizational level. An organizational unit assumes the identity of an operational FC as it develops the capabilities necessary to support the receipt, analysis, gathering and dissemination of threat information. The longer the organization operates with these capabilities, the more other government agencies and the public come to take it for granted as a member of the FC category. Thus the identity of each Fusion Center emerges both within its geographic and administrative locality and at the national level. Similarly, personal identities (roles) of staff are circumscribed by their professional skills: as analysts continue to interact with the information sources and databases, and as they produce their products over time, the taken-for-grantedness of their professional identities deepens and their professional identities emerge.

Legitimacy occurs with regard to standards, norms, and boundaries – especially around categories and identities – and is primarily established at broader societal levels, such as state-level and federal government agencies (in terms of legislation and resource provision), as well as via major press and national media. Heightened legitimacy can be seen in the history of
published materials (e.g. FC Guidelines 2006; Baseline Capabilities 2008; Critical Infrastructure and Key Resources Protection Capabilities for FCs 2008; 2010 Baseline Capabilities Assessment).

While numerous self-reinforcing dynamics are at play, this paper highlights two aspects in particular that seem especially significant in these change processes over time: institutional logics and influence of a central agency.

Institutional Logics

The concept of institutional logics was first introduced by Friedland and Alford (1991). They write:

Each of the most important institutional orders … has a central logic – a set of material practices and symbolic constructions – which constitutes its organizing principles and which is available to organizations and individuals to elaborate. …. These institutional logics are symbolically grounded, organizationally structured, politically defended, and technically and materially constrained....

Thus institutions are symbolic systems which have nonobservable, absolute, transrational referents and observable social relations which concretize them. (1991:248-249)

The concept of “information” and how “it” is “processed” can thus be understood as an institutional logic. The central institutional logic (Friedland and Alford 1991) of FCs revolves around the receipt, analysis, dissemination and gathering of “threat information.” FC organizational practices and symbolic constructions are technologically enabled and constrained by sophisticated combinations of interoperable technologies and cross-boundary practices materially grounded in the use of databases and communication networks. The fundamental attributes of these databases are categories: professional practice entails “knowing” how to manage data and databases according to specific sets of rules and heuristics that comprise a set of professional analytical skills through which the data in databases is transformed into “actionable knowledge” (FC Guidelines 2006). For example, one simple practice involves the cross-referencing of data records according to a single attribute, e.g. matching a license plate number or social security number across different databases to track the identity of a “suspected terrorist.”

Performing such practices establishes an analyst’s identity and constitutes the capability defining the identity of a FC; at the same time, performance also sediments the relevant categories (e.g. “threat,” “terrorist”) in the analyst’s and professional community’s memories. For example, investigating a Suspicious Activity Report (SAR) – a standard category – deepens the taken-for-grantedness of the categories of “suspicious activity” and “terrorist” for analysts; concurrently it helps to constitute the capabilities and identity of the individual FC. Furthermore, because the form is standardized and other FCs are handling the same form in the same way (FEMA National Preparedness Report 2012: 14), the SAR-based practice also heightens the legitimacy of the organizational field among its constituent organizations (FCs).

Nevertheless, a collection of heterogeneous FCs would not emerge as an organizational field if their core identities and key categories did not also achieve legitimacy in the broader society. And achieving this legitimacy is not a foregone conclusion. Indeed, public concerns about the broadening of law enforcement and intelligence capabilities for domestic surveillance that impact upon privacy and civil liberties issues, and the “mission creep” that Regan and Monahan (2011) refer to, have resulted in opposition to the growth and legitimization of FCs. In response, FCs have started issuing public reports that feature their organizational efficacy at catching criminals, obtained through sharing information across jurisdictional boundaries; a public relations strategy that aligns an FC with the institutional logic of other local agencies in neighboring organizational fields (e.g. police and sheriffs), as a means of bolstering their legitimacy.

Influence

As with organizational fields more generally, the emergent field of FCs naturally co-evolves with and is influenced by other organizational fields and agencies (DiMaggio 1991). One such neighboring field comprises technology sector firms that develop and market surveillance technologies (e.g. face and license plate recognition, cellphone locators) and large database management and analytic technologies (e.g. big data aggregation technologies and pattern detection analytics). Other co-evolving fields are comprised of political and legal organizations, including the US Congress and oversight committees, and public interest groups concerned with civil liberties and privacy, such as the American Civil Liberties Union and The Constitution Project.

In addition to these cooperating and competing neighboring fields, some federal level agencies have formal authority over the emergent organizational field of FCs. Through accepting the rules and guidance – such as the FC Guidelines (2006) and Baseline Capabilities (2008) – that have been developed and distributed by federal agencies, FC staff come to take their FC roles and identities more for-granted. Federal agencies also elicit public support of FCs’ mission indirectly, through the national “See Something, Say Something” campaign (http://www.dhs.gov/if-you-see-something-say-something-campaign), posting authoritative signs in public places such as mass transit and sports arenas encouraging citizens to report “suspicious”
behavior; tips are then channeled via SARs and the National SAR Initiative (NSI) (NSI 2013; PM-ISE 2008, 2011) to local FCs for investigation. Regular use of the SAR form mandated by the Federal-level Program Manager for the Information Sharing Environment (PM-ISE) (NSI 2008, 2013) then sediments the SAR’s taken-for-grantedness, bolstering it as a key institutional category (while at the same time strengthening analysts’ professional and FCs’ organizational identity).

One “central agency” (DiMaggio 1991) appears to have had an especially supportive role in this emergence of the FC organizational field: the US Department of Homeland Security (DHS) has been facilitating the deepening taken-for-grantedness and the heightened legitimacy of the FC organizational field in multiple, mutually-reinforcing ways.

This central agency assists with the deepening taken-for-grantedness of identities in a variety of ways. Most FCs have depended upon funding received from DHS for sustaining their daily operations (PM-ISE 2011; US Senate 2012); without such operational support, analysts and directors would likely not be practicing their roles and assuming their respective identities. DHS also provides highly skilled analysts, serving as role models for the new population of FC analysts. The analytic training and operational funding thereby engender career aspirations of FC personnel based upon these identities, feeding back into the institutionalization of the organizations and the field. Additionally, DHS supports FC conferences, trainings and exercises that are important for configuring the emerging organizational field (Garud 2008), and exercising professional identities, further deepening their taken-for-grantedness.

Legitimacy is heightened via a number of different routes by federal-level agencies. Through the published guidance that DHS and DOJ provide to FCs, these agencies influence the establishment of norms of professional (analyst) behavior and of standard categories such as threat, terrorist and SAR. DHS and DOJ have also had indirect influence on FC norms and standard categories through provision of trained analytical staff to work in the FCs (Public Intelligence 2011; FEMA/DHS 2012), and DHS has been instrumental in assessing and certifying FC capabilities (Abold, Guidetti & Keyer 2012; DHS 2013a).

Additionally, DHS mediates FC relationships with many other “external” entities, including private sector organizations. And through their testimony to Congressional committees, DHS officials seek funding for FCs; DHS then makes determinations about how funding is distributed among the states which then channel portions of that funding to the FCs. And through the Critical Infrastructure and Key Resources (CIKR) program under DHS’ Office of Infrastructure Protection, DHS mediates FC relationships with government agencies and private sector organizations responsible for safeguarding societal infrastructure resources such as power plants, transportation and communication resources (CIKR Protection for FCs, 2008).

**Contestation**

As noted above, emergence of FCs and of the FC organizational field has been contested in public arenas by public interest organizations concerned with privacy and civil liberties issues. In response to the extension of domestic surveillance capabilities funded out of taxpayer dollars and implemented by FCs, protests have arisen. Still, US Government oversight has been relatively restrained, as noted in the recent report released by the US Senate’s Permanent Subcommittee on Investigations of the Committee on Homeland Security and Governmental Affairs (2012). The relative weakness of this contestation is perhaps surprising – had public protest been more strident, the field’s institutionalization might not have been successful.

This weakness of contestation may be due in part to the secrecy surrounding FC development and operations. Although the number and capabilities of FCs have grown substantially over the past decade, they are largely invisible to the public. DHS’ Intelligence & Analysis (I&A) arm, an organization not generally well-known because much its work is classified, has played the major role with regard to the maturation of FCs (Abold, Guidetti & Keyer 2012; CIKR Protection for FCs 2008; FEMA NPR 2012). Many FCs are housed in unmarked locations or buildings that bear another agency’s name; some do not reveal their street address at all. And despite the press coverage that often accompanies the opening of a FC, day-to-day operations and capabilities – i.e. much of the emergent field – remains largely hidden from the public view.

**CONCLUSION**

**Theoretical implications**

This paper has described the emergence of a new organizational field that accompanied the development of networked technology for information sharing, the combination approaching a true infrastructure. The paper has highlighted two phenomena of particular importance relative to this institutionalization. One is the influence of a central agency (DiMaggio 1991) that fuels multiple, self-reinforcing dynamics that deepen the taken-for-grantedness and heighten the legitimacy of organizational categories such as SARs, and professional identities such as “analyst.” The other is an institutional logics perspective which draws attention to how the emergence of the field is supported by the development of technologies which
enable and constrain powerful capabilities for managing categories of persons and their behaviors. This suggests that institutional theory may be a significant source of insights for the developing field of infrastructure studies.

Practical implications
The emergent field of FCs is one of several such organizational fields developing in the same timeframe; others include the Nationwide SAR Initiative (NSI), the Emergency Management organizational field (DHS-DOJ Comprehensive Preparedness Guide (CPG) 502, 2010), and the National Infrastructure Protection Plan, which partners with private sector firms in 18 critical infrastructure sectors through mechanisms such as FBI’s InfraGard program (NPR 2012) and DHS’ CIKR program. Federal agencies in general – and DHS in particular – therefore appear to be supporting the emergence of an institutional field and strengthening their own position through their combined influence over several emerging organizational fields in mutually reinforcing ways. As noted by Barbara Neuby in a paper titled “Bureaucratic Power: Security and the National Response Plan” (2006: 317) it appears that the US Department of Homeland Security (DHS) has “skillfully used its sources of administrative power to build a latent control network, with little or no oversight, raising questions of accountability and ultimate security.” Other scholars have also warned about the ability of small, relatively invisible groups, to exert influence over emergent institutional phenomena. Steve Barley (2010) notes that it is possible to “buil[d] an institutional field ... to exert greater influence on [government agencies]... while simultaneously shielding the [instigators] from appearing to directly influence [those agencies].” Zald and Lounsbury (2010) propose an institutionalist agenda to study how hidden elites and their “command posts” are able to shape the dynamics of economy and society.

Research implications
These theoretical and practical implications point to important areas for future research. Yet data collection in support of such research faces a unique set of challenges. Researchers at the Washington Post conducted an investigation into the vast growth of US secret and top secret operatives and bureaucracy over the past decade. Their findings (2010), indicate that much of the funding for the growth of this larger enterprise, including DHS/I&A and FCs, is “black” – i.e. untraceable and unaccountable. It may therefore be impossible to determine how much funding and capability actually support the emergence of an organizational or institutional field and/or for what ultimate purpose. Yet further research and public concern are not only important and timely but essential for understanding the true nature and implications of this emergent information infrastructure.

ACKNOWLEDGMENTS
Background knowledge about Fusion Centers was gained through employment with The MITRE Corporation, and the “Exploring DHS Fusion Centers” research project (US National Science Foundation grants SES-095707, SES-0957283; directed by Torin Monahan and Priscilla Regan). The data collection and analysis reflected in this paper were developed independently, more than 18 months after separating from those organizations and terms of employment. I thank Torin, Pris, and Dean Roger Chalkley for their support and encouragement around my bringing this research interest to fruition.

REFERENCES

Official Fusion Center Documents


**Additional References**


