Towards Permeable Boundaries of Organizations?

Big Data, Bigger Questions: Data-based Business Models and Their Implications for Organizational Boundaries, Data Governance, and Society

Angelique Slade Shantz,

BIG DATA, BIGGER QUESTIONS: DATA-BASED BUSINESS MODELS AND THEIR IMPLICATIONS FOR ORGANIZATIONAL BOUNDARIES, DATA GOVERNANCE, AND SOCIETY

Angelique Slade Shantz

ABSTRACT

Access to personal data is key to many of the most successful recent business models. These models rely on individuals outside of traditional organizational boundaries as their product, content providers, and customers. The topic of organizational boundaries is central to organizational research, and these models raise questions about the permeability of these new forms' boundaries. Herein I elaborate on data-based business models, the organizational field that has emerged around data governance issues, and the institutions that have formed around it at different stages, by various actors. I also explore the interplay of institutional field and organizational boundaries, to identify how field-level issues influence the permeability of organizational boundaries.

Keywords: Organizational boundaries; emergent institutional fields; data-based business models; big data; boundary permeability; data governance

Toward Permeable Boundaries of Organizations?
Research in the Sociology of Organizations, Volume 57, 305−329
Copyright © 2018 by Emerald Publishing Limited
All rights of reproduction in any form reserved
ISSN: 0733-558X/doi:10.1108/S0733-558X20180000057012

INTRODUCTION

> If something is free, you're not the customer; you're the product … We're not the customers. We're products those companies sell to their real customers. (Schneier, 2015)

Access to large swaths of personal data is the backbone of many of the most successful business models of the past two decades (Culnan & Armstrong, 1999), and it is increasingly difficult to engage in modern life without allowing one's personal data to be digitized, as many of the free or "freemium" services that we come to rely on are predicated on a *quid pro quo* business model of service-for-data (Brunton & Nissenbaum, 2011). To provide a sense of the magnitude of this phenomenon, users post around 95 million "tweets" per day, and approximately 30 billion pieces of content on Facebook per month (Pentland, 2011). The data of the individuals engaging in these interactions are sold, resulting in approximately US$75 billion of personal information provided to consumer marketers annually (Schwartz, 2004). In short, these business models rely on individuals outside of traditional organizational boundaries (users) as their product (data), content providers (posts), and customers (consumers of content and advertising). This raises a wide range of questions about traditional organizational forms and the increasingly permeable boundaries of these new organizational forms (CfP, Towards Permeable Boundaries of Organizations). These new forms and the permeability of their boundaries also have significant implications for society, most notably how data, widely considered to be the "new currency of the digital world" (Meglena Kuneva, 2009, as quoted in Pentland, 2011), are governed.

The topic of organizational boundaries is central to organizational research, and its study has typically been dominated by the theoretical lenses of transaction cost economics (TCE) and related exchange-efficiency perspectives (Nickerson & Silverman, 2003; Poppo & Zenger, 1998; Santos & Eisenhardt, 2005a, 2005b; Williamson, 1975, 1981), with concerns related to "make" versus "buy" decisions, and considerations of governance mechanisms such as strategic alliances, joint ventures, and contractual arrangements (Afuah, 2003). Traditional conceptualizations of what falls within organizational boundaries include elements such as a hierarchy of decision-makers who make decisions on other members' behalf, for example, related to who membership includes, how to allocate resources, and how to monitor and enforce the rules these decision-makers have made (Ahrne & Brunsson, 2011). More recently, scholars have begun to explore whether and how organizational boundaries may be more permeable than initially conceptualized, as firms are held to higher standards of accountability and must therefore open their boundaries to public scrutiny (Hood, 2006), operate more frequently as members of a broader network (Ahrne & Brunsson, 2008, 2011), and include a wider range of stakeholders in their planning processes and decisions (Zietsma & Lawrence, 2010). These shifts are often driven in response to field-level concerns, arising through pressures from field-level actors such as trade associations (Buchanan, 2016), customers (Scaraboto & Fischer, 2013), and activists (Briscoe, Gupta, & Anner, 2015), particularly when fields are emerging (Maguire, Hardy, & Lawrence, 2004; Purdy & Gray, 2009). Yet, less theoretical attention has been given to how emerging institutional fields, and the actors, events and institutions that constitute them, influence the boundary permeability of the organizations that reside within them. While it has been acknowledged that technology and the Internet generally, and the "digital age" more specifically, does call into question many of the assumptions of more traditional organizational boundaries research (Afuah, 2003; Powell, Oberg, Korff, Oelberger, & Kloos, 2016), we know little about how the emergent institutional field which has formed around the phenomenon of data-driven business models may have shaped the boundary permeability of the organizational actors in its membership. More specifically, if organizational boundary research is concerned with make versus buy decisions and the governance mechanisms that facilitate them, then data, described as a "new asset class," characterized by ambiguous ownership (Pentland, 2011), those individuals who provide it to organizations, and the governance of these transactions, may provide fresh, phenomenon-driven (Schwarz & Stensaker, 2014) insights into the study of organizational boundaries.

Here, I use an institutional lens to explore the development of an organizational field centered around the issue of digital data and its governance, the evolving institutions adopted by firms whose business models are predicated on access to data as a major input and primary organizational asset, and its effects on organizational boundary porosity. By governance, I refer to both field-level governance, that is, the mechanisms that uphold the "rules of the game" within a field (Zietsma, Groenewegen, Logue, & Hinings, 2016), as well as firm-level governance, which is concerned with transactions among trading partners. Organizational fields have been defined as organizational clusters whose boundaries are defined and stabilized by shared logics (Greenwood & Suddaby, 2006, p. 28; see also Scott, 1995), or united by a key issue set (Hoffman, 1999), or "issue field" (Hoffman, 1999; Zietsma et al., 2016). While governance mechanisms in an established field are institutionalized, characterized by routinized interactions between participants, and a stable set of field participants (Greenwood & Suddaby, 2006), emerging organizational fields may be characterized by institutional voids, governance gaps, and a fluctuating set of actors (Maguire et al., 2004). The relative newness of the organizational field of interest here provides a unique opportunity to better understand how new institutions, particularly those surrounding governance mechanisms, develop in a new industry and organizational field, and how this in turn influences the ambiguity or permeability of organizational boundaries.

In summary, a combination of technological change, new business models, and changing legal frameworks, have created a new phenomenon, accompanied by a host of tensions and complexities. The subsequent analysis attempts to shed light on the governance of the data that is emerging from this novel context, which is said to fall into a "governance gap" (Egels-Zandén & Hyllman, 2006). This issue of data governance, or lack thereof, is particularly germane to firms whose business models are predicated on access to large amounts of personal data as their primary activity and asset. Therefore, the focus of the following analysis is on the industry comprised of companies, such as Google, Facebook, and Twitter, to name just a handful of the most prominent, whose *primary* activity is the use (sale, sharing, analysis, etc.) of the data of its users, and the organizational field that has emerged around issues related to the governance of data in this industry. I ask the following research question: How did the emergent institutional field of data governance influence the permeability of organizational boundaries in the data-based business industry? In so doing, I make several contributions. First, I trace the development of an emerging field centered around the issue of digital data and their governance, and simultaneously explore the evolving data governance institutions adopted by firms whose business models are predicated on access to data as a major input. In so doing, I highlight how fields affect the porosity of organizational boundaries, and determine what side of organizational boundaries actors fall on. Finally, I provide definitional clarity and boundary conditions around an emerging yet opaque and under-studied (yet theoretically generative) phenomenon, which will hopefully provide a foundation for future academic inquiry, and enhance theoretical understanding of organizational boundaries in light of novel organizational forms and models. Addressing this phenomenon through the approach of a "problem-driven boundary phenomenon" also responds to calls to allow contemporary boundary issues and alternative theoretical lenses to drive new advances in the study of organizational boundaries (Santos & Eisenhardt, 2005a, 2005b). I will begin with a brief introduction to the phenomenon of interest and its relationship to organizational boundaries, then explore the key issues and key actors (Hoffman, 1999) that shape digital data and its governance as an organizational field. I will next move on to an institutional history of data governance, and the formative stages and disruptive events that have shaped its emergence, and end with a discussion and conclusion.

DATA-BASED BUSINESS MODELS AND ORGANIZATIONAL BOUNDARIES

The rise of business models that rely on personal data for their primary activity, sometimes referred to as the "attention economy" (Pentland, 2011), has become an increasingly prominent feature of the modern economic landscape. Yet, despite the magnitude of this phenomenon, rigorous definitional parameters remain opaque and contested. Scholarly inquiry into this domain yields a fragmented cluster of discussions, from a broad range of academic fields, each approaching the study of digital data and their governance through various lenses and at various levels. The legal literature has largely approached the topic from a macro or state level, often taking a comparative methodology to highlight differences in particular between the US and EU's approach to data governance (see, e.g., Reidenberg, 2000; Schwartz, 2013), whereas, the communication literature has tended to focus (often critically) on the governance of the Internet and cyberspace rather than data (see, e.g., Deibert & Rohozinski, 2010a, 2010b; DeNardis, 2013), as well as approaches that individuals take to reclaim the governance of their data, such as obfuscation (Brunton & Nissenbaum, 2011; Howe & Nissenbaum, 2009) and hacking (Coleman, 2013). The communication and business ethics literatures have largely addressed the topic from the perspective of the producers of data (i.e., the users of the Internet and affiliated tools and resources and "generators/owners" of data) (see, e.g., Byrne, 1996) whereas the medical literature is predominantly data focused, but spanning both the producers and owners of the data (i.e., patients), as well as the users of the data (i.e., physicians and researchers), and tradeoffs between the use of patient data in improving healthcare and the dangers of ethical violations related to patient privacy.

Given this fragmentation, I begin with a definition to delineate my industry of interest, which I will refer to in what follows as data-based businesses (DBBs): *Firms or business units who capitalize on the growing monetary value of personal data via business models that depend on the collection, storage, aggregation, and mining of personal digital data, typically for the tracking and targeting of users, typically for the ultimate purpose of online behavioral advertising (OBA).*[1] By business model, I refer to the set of strategic choices surrounding how an organization will create and deliver value for its key constituents, such as how it will generate revenue streams, identify and attract customers, and manage relationships and partnerships with stakeholders (Ocasio & Radoynovska, 2016). By personal data, I refer to digital data created by and about people, including profile and demographic data from bank accounts, medical records, employment data, recorded preferences from web searches and sites visited, clicks, purchases, likes and dislikes, tweets, texts, emails, phone calls, photos, videos, and geographic coordinates (Pentland, 2011). These data can be loosely bucketed into three types: volunteered data such as social network profiles, which is typically created and shared by individuals; observed data such as cell phone-derived location data, which is captured by recording the actions of individuals; and inferred data, such as credit scores, which is inferred by the analysis of volunteered or observed data (Pentland, 2011). This is often broadly referred to as big data, although its defining characteristic typically emphasizes relationality – that is, the patterns that can be derived from connections between pieces of data – rather than quantity (Boyd & Crawford, 2012).

One particularly complex aspect of this industry as it is defined above is the fuzziness of the boundaries of the industry itself, and its relation to several subindustries. For some of these sub-industries, it is not yet clear whether their primary focus is data or services, and they are often typified by opacity in the source of their economic value. Included in this category are wearable technology companies, such as Fitbit and Jawbone UP. Wearable technology firms, while currently selling a product, are poised to be hubs for vast amounts of personal data, and it is as yet unclear whether the data will eventually surpass the product in value and import to these firms. Another example of this is a subset of the so-called "sharing economy," with firms such as Uber and AirBnB. The sharing economy is typified by business models that feature power shifts from large firms to distributed networks, and disintermediation, or the elimination of middlemen to capture efficiencies (Botsman, 2013). While the boundaries of what the sharing economy actually entails remains contested (Acquier, Daudigeos, & Pinske, 2017), there is some consensus that it relies heavily on the power of digital technologies (Acquier et al., 2017; Belk, 2014). Moreover, while they appear to be providing a service while finding efficiencies in the system through the elimination of middlemen, the large amounts of data they collect may in the future surpass their current service-provision functionality for primacy. More generally, while early Internet advocates heralded the elimination of traditional corporate intermediaries, those who now control the flow of information and data between buyers and sellers, have become powerful middlemen themselves (Schneier, 2015). In addition, while firms such as Google and other search engines or Facebook and other social media sites are more explicitly considered to be DBBs and therefore subject to more public scrutiny, others, such as rewards programs of credit cards or grocery stores, are better able to utilize data in ways that avoid users' scrutiny. However, each has in common that users, while undoubtedly reaping benefits from the use of the service, are not customers in the traditional sense, as their data are, in some transactional form, sold to an end customer.

The above discussion highlights several key features of how this phenomenon calls into question organizational boundaries. First, when organizations rely on business models that derive value from individuals' data outside of the organization, it becomes unclear who the members of an organization are. Second, when the rules around who "owns" said data are as yet undetermined, it is also unclear whether these important assets (often considered to be these organizations' primary assets) reside within or outside of the organization. Finally, when field membership is ambiguous, it is also unclear what rules pertain to what types of organizations.

DATA GOVERNANCE AS AN ORGANIZATIONAL FIELD

While institutional or organizational fields have been defined in a wide variety of ways, here I follow Hoffman's (1999) conceptualization, which foregrounds issues, actors, and field-configuring events (Anand & Watson, 2004;

Hardy & Maguire, 2010; Schüssler, Rüling, & Wittneben, 2014), suggesting that fields are dynamic, and form

> … around a central issue … [and] become centers of debates in which competing interests negotiate over issue interpretation. As a result, competing institutions may lie within individual populations (or classes of constituencies) that inhabit a field. (Hoffman, 1999, p. 351)

More recently, power dynamics and struggles have come to feature prominently in discussions of fields (Meyer & Höllerer, 2010; Zietsma et al., 2016). This description highlights the distinction between issue fields, which is closely aligned with Hoffman's conceptualization, and exchange fields, which are more stable, and contain clusters of "populations," or industries, with stable relationships, norms, and practices (Zietsma et al., 2016). Drilling down even further, issue fields can be "interstitial" (Rao, Morrill, & Zald, 2000) in nature, drawing members from pluralistic logics and multiple fields, but likely to settle into exchange fields over time; or they can be "bridging" in nature, also pluralistic but unlikely to settle into stable exchange fields because they are transnational (Buchholz, 2016) or otherwise cross-jurisdictional (Zietsma et al., 2016). Relatedly, fields can vary in their degree of institutionalization, and can be emergent, characterized by low levels of institutional infrastructure, or stable and mature, with settled, self-reinforcing institutions (Greenwood, Suddaby, & Hinings, 2002; Hinings, Logue, & Zietsma, 2017). In summary, if organizational fields are indeed formed around the issues that are pivotal to the interests and objectives of a set of organizations (Hoffman, 1999), then a first important task in understanding the emergent organizational field of data governance in the context of DBBs is to identify, based on a systematic review of relevant literature, the key issues and various responses to them, as well as the key actors involved.

Key Issues

In what follows I outline the issues considered to be central to this organizational field; that is, issues related to ownership, privacy, tracking and discrimination, and power and democracy.

Data Ownership: At a broad level, questions around who owns the data and the rights that accompany this ownership are at the heart of the tension inherent in DBB models; that is, "how much value will ultimately be created, and who will gain from it" (Pentland, 2011). From an organizational boundaries perspective, if the ownership of the key assets of an organization (that is, data) is ambiguous, possibly residing at least partially with the individual the data pertains to, this presents significant practical and theoretical complexities. Most scholarly perspectives (primarily from the legal domain) suggest that ownership perspectives are contingent on factors such as data type, information type, institutional regime, and firm type. For example, one distinction is between raw (unworked) data, which is said to belong to no one, and refined (worked) data, which is said to belong to the collector or those the collector grants access to (Byrne, 1996). From this perspective, once a firm "adds value" to raw data through analysis, ownership is transferred to the firm. Another perspective is that different classes of information, such as financial, health, government records, and social data, are afforded different degrees of protection (Pentland, 2011). For example, the ownership of health and government records may be protected more stringently than social data (although some perspectives suggest that analysis of patterns in social data can reveal as much if not more than self-reported data such as that found in heath records, calling into question the validity of this distinction). A third perspective compares a human-rights-based approach to privacy, which has been the general perspective of the EU, to the more hands-off approach followed by the US (Victor, 2013). From this perspective, where the data originate will determine how and the extent to which its ownership is protected, although questions related to the relative importance of the firm location versus the location of the individual whose data are collected remain unclear. A fourth perspective suggests a distinction at the firm level as to how data ownership will be viewed, whereby firms with significant information assets follow a logic that views data as a private good, whereas firms with few information assets promote a liberal data policy ideology (Newman, 2010). Most perspectives suggest that while the matter of ownership would appear to be a simple one, and that individuals should own their own data and be able to control how it is used and by whom, the underlying issues are so complex that many advocate that approaches related to "rights management" are a more productive avenue than ownership given the nature and stage of the data governance debate (Pentland, 2011).

Data Privacy: In this chapter, I follow Schwartz' (2004) definition of information and data privacy as "the result of legal restrictions and other conditions, such as social norms, that govern the use, transfer, and processing of personal data" (p. 2059). Because of the *quid pro quo* nature of many of the DBB models whereby personal data are considered to be the "fee" paid for many online services, a widely held norm among DBBs is based on a basic utility argument, such that if users are informed of practices related to the collection and use of personal information, individuals may then decide if the "price is right"; also referred to as "transparency and choice," "notice and consent," or "informed consent," whereby data policies are explicit and the option to engage or disengage is provided (Nissenbaum, 2011). The norm regarding the choice to engage or disengage currently follows an "opt out" rather than an "opt in" logic, although many suggest that the legal and ethical basis for this is contested, given that "the price of not engaging socially, commercially, and financially may in fact be exacting enough to call into question how freely these choices are made" (Nissenbaum, 2011, p. 35). Policies that focus on notice are also considered problematic due to the legalistic and inaccessible nature of the policies, as well as online entities' right to change the policies at will. This requires that consumers of online services who wish to fully comprehend the extent of the implications of their online interactions must read (and comprehend) every online provider's policies not once, but repeatedly (Nissenbaum, 2011). This has significant implications for organizational boundaries, because while most organizations are facing increasing demands for transparency (Hood, 2006; CfP), the norms around data governance have remained highly ambiguous and opaque. This is in stark contrast to the fact that users are becoming ever more transparent to the organizations that service them.

Data-based Discrimination, Democracy and Power: Tracking, the capture of online behavior and information, allows for the equally widespread practice of targeting. Targeting is the differential selection of ads based on interests, dispositions, preferences, propensities, weaknesses, past behavior, and any other information that can be gleaned from online tracking (Barocas & Nissenbaum, 2009). While the relative annoyance or utility of targeted advertising is widely debated, the more complex issues in question among scholarly debates are the discriminatory repercussions of the "panoptic sort" (Gandy, 1993), that is, the practice of assigning advertising "treatments" to different categories of individuals based on aggregated data, or "surveillance as social sorting: a means of verifying identities but also of assessing risks and assigning worth" (Lyon & Burton, 1995, p. i, as cited in Andrejevic, 2014). Recent technological advances expand these implications to include not only data-based differentiation, but also prediction, based not on who an individual is in the present, but on future actions and desires. (Gandy, 2005, p. 3). As one example, a 2012 study used cell phone data alone to predict, within 20 meters, where individuals would be in 24 hours (Schneier, 2015). When taken to its extreme, this previews a future of organizations that can identify their customers' weaknesses and vulnerabilities by closely monitoring past behaviors and dispositions, information which may then be used to actively shape choices, actions, transactions, and purchasing decisions (Barocas & Nissenbaum, 2009). These issues have important implications for the role of the firm not only in meeting customer demand, nor even in predicting customer demand, but in shaping customer behavior, with more precision and control than has been historically possible in the absence of such large, precise, and longitudinal amounts of data.

The issues surrounding both tracking and targeting lead to larger questions of power that go beyond issues related to the collection and use of personal information (Andrejevic, 2014), given that in many cases "opting-out" of online life is not an option, and that even with notice or transparent privacy policies, users may not fully understand the implications of their online actions. Moreover, Andrejevic (2014) points to the technological and infrastructure-related power that unlocks both the benefits and costs to society of big data:

> the era of big data—characterized by the ability to make use of databases too large for any individual or group of individuals to comprehend—ushers in powerful new capabilities for decision making and prediction unavailable to those without access to the databases, storage, and processing power. (p. 20)

As an example of this link between data and democracy, the well-known online petition platform "Change.org" is used by millions of users, both to start and sign petitions. A less well-known aspect of their platform is the business model that drives it:

> We fund our free global empowerment platform by accepting advertising in the form of sponsored petitions, similar to sponsored videos on YouTube, sponsored links on Google, or sponsored tweets on Twitter…This is a form of "cost-per-action" advertising, which is common among online platforms. (change.org website)

Therefore, users who do not want their data sold to advertisers with "sponsored" petitions must opt out of signing online petitions made via the Change.org platform.

The above issues, particularly related to democracy and power, raise questions about the boundaries of firms' power; that is, what is the appropriate sphere of organizational influence as it relates to how organizations control the exchange relations in which their organization is involved (Santos & Eisenhardt, 2005a, 2005b). In the context of DBBs, organizations essentially outsource the product to external actors; that is, individuals provide their data and "attention," which becomes the product that organizations sell to customers (advertisers). Simultaneously, individuals provide the content that entices other individuals to give their attention (and thus their data). However, the ambiguity of data ownership introduces significant uncertainty to firms in their desire to control resources, raising questions about the sustainability of this boundary configuration (Pfeffer & Salancik, 1978; Santos & Eisenhardt, 2005a, 2005b). However, in ambiguous environments, organizations have been suggested to act offensively to capture market value (Ozcan & Eisenhardt, 2005), therefore DBBs may be using the lack of field settlement (Helms, Oliver, & Webb, 2012) and ambiguity of this organizational field to shape this emergent market in their favor (Santos & Eisenhardt, 2005a, 2005b). More specifically, the implications highlight the theoretical benefits of "a *permeable* view of boundaries that includes both ownership and non-ownership mechanisms" (Santos & Eisenhardt, 2005a, 2005b, p. 497) as a way to enhance firms' strategic flexibility and extend their sphere of influence without extending their legal boundaries (Pfeffer & Salancik, 1978; Santos & Eisenhardt, 2005a, 2005b). Organizations find non-ownership mechanisms (such as board appointments, alliances, lobbying) to be particularly valuable in ambiguous or dynamic environments or when the size of the organization renders ownership-based strategies (such as mergers and acquisitions) sub-optimal (Santos & Eisenhardt, 2005a), such as is often the case in (particularly young) technology firms.

Key Actors

With key issues identified, it then becomes critical to understand who the key actors in this organizational field have been, and will be in the future

(Greenwood, Hinings & Whetten, 2014). This is particularly important in a nascent industry and organizational field whereby any one key actor may have more power and voice than a single actor participating in a larger or more developed field (Maguire et al., 2004). At the field level, key actors include individuals, firms, and the government/public sector, however, a more meaningful distinguishing dimension in the discussion of organizational boundaries is between the producers and consumers of data, as well as between internal and external actors in the typical DBB.

In traditional DBB models, individuals are the producers (i.e., sources or subjects) of personal data, sometimes in exchange for free services. As described by Schneier (2015), "If something is free, you're not the customer; you're the product … . We're not the customers. We're products those companies sell to their *real* customers" (p. 53). Individuals, firms and the public sector can all be classified as consumers of personal data. Although firms have typically been considered to be the most important consumers of data via DBB models and in other ways, governments are becoming increasingly sophisticated in harnessing personal data to achieve societal aims (Pentland, 2011), such as big data-derived insights that are frequent in the medical field, and surveillance data which has growing prominence in criminal investigations (Schneier, 2015).

In addition, despite claims that the power to analyze data is consolidated in large firms (Andrejevic, 2014), individuals are increasingly empowered to glean meaningful insights from their own data. Take, for example, the nascent "quantified self" movement, motivated in part by developments in wearable technology. This movement, defined by individuals collecting and analyzing their personal data (e.g., sleep, steps, or biometric data), has been characterized as a form of "soft" resistance to dominant modes of interactions with big data within the boundaries of organizations, in ways that circumvent a system of powerful big data institutions designed around advertisers rather than users (Nafus & Sherman, 2014). This "soft resistance" is so described because it reflects an agentic choice that individuals make to collect and analyze their own data, outside of traditional organizational boundaries, by assuming:

> … multiple roles as project designers, data collectors, and critical sense-makers, rapidly assessing and often changing what data they collect and why in response to idiosyncratically shifting sets of priorities and objectives … and thus creates both material and social resistance to traditional modes of data aggregation. (Nafus & Sherman, 2014, p. 1785)

What falls within the typical DBB firm boundary is an intermediary or "data broker" function (Schneier, 2015), also referred to as ad networks and ad exchanges. Ad networks utilize users' interests and preferences inferred from historical browsing behaviors, accumulated from the ability to track users' online behavior as they navigate and engage with sites, to provide them with highly targeted ads (e.g., Google's Ad Sense, AOL's TACODA, Microsoft's Atlas, and Yahoo's Right Media). Distinct from context-dependent advertising, which present users with ads based on one-off search queries (sponsored searches), ad networks act as an outsourced third party that follows users across sites to bridge groups of online publishers and advertisers, so that advertisers can buy ad space across a network of online publishers, with richer and more detailed user profiles, and allow the ad network to use that data to select the most appropriate ad for a particular user on a particular site (Barocas & Nissenbaum, 2009). Ad exchanges are a market place for the "purchase and sale of impressions," functioning as a platform for transactions among various kinds of market participants, including but not limited to ad networks. While providing a transparent and efficient platform for online behavioral advertizing-related data purchase, this platform also introduces further complexity to transactions related to user data by replacing stable contractual B2B data sales arrangements with a data auction platform (Barocas & Nissenbaum, 2009).

Institutional History

Next, I present an institutional history of the organizational field of data governance as it relates to the DBB realm, as described by Table 1, which includes key events and time periods in each of three stages. The emergence of data governance has followed three stages, differentiated by disruptive, field-configuring events, resulting in changes in the organizational field, and institutional shifts, each with implications for the boundaries of organizations (Table 2).

Stage 1: Pre-regulatory. The 1990s, typically labeled as the dot.com boom, the dawning of the Internet age, and Web 1.0 (retrospectively), was the decade in which the World Wide Web was born, and a host of Internet heavyweights, such as Yahoo, eBay, napster, and Google, were founded, before the dot.com

Table 1. Key Actors.

Actor	Role	Producer/ Consumer	Internal/External to Firm Boundaries
Individual	• Provides personal data via use of services (e.g., "likes" something) • Provides content that entices users (e.g., "posts" a picture) • Consumes content that others provide (e.g., "clicks" on a link) • Uses own and other personal data (e.g., analyzes performance, compares against others for motivation or information)	• Producer of data • Producer of content • Consumer of content • Consumer of data	• External • External • External • External
Firm	• Provider of platform • Data Broker (e.g., Ad Networks/ Exchanges) • Advertiser, e.g., online publishers	• Intermediary • Intermediary • Consumer of data	• Internal • Internal • External

Table 2. Institutional History.

Stages	Stage 1: Pre-regulatory Approach (early- to mid-1990s)	Stage 2: Regulatory versus Normative Approaches (mid-1990s to mid-2000s)	Stage 3: Cognitive and Individual Approaches (mid-2000s onwards)
Key Events	• 1990: www, Web 1.0 "born" • 1994: Yahoo founded • 1995: Start of .com bubble; eBay & Amazon founded	• 1995: FTC under pressure to oversee data/privacy issues • 1998: EU's Data Protection Directive; Google founded • 2000: EU/US agree on Safe Harbor Principles; burst of .com bubble • 2001: DoubleClick case dismissed; USA Patriot Act enacted; Wikipedia founded • 2002: Linked In founded • 2004: Web 2.0 born, Facebook founded • 2005: YouTube founded • 2006: Twitter founded	• 2006: AOL discloses search queries of 650,000 users; TrackMeNot made freely available • 2011: Max Schrems demands data from Facebook, files court case • 2012: Release of General Data Protection Regulation
Boundary Shifts	Broader boundaries encompassing internet governance supersede firm-level data governance issues; governance dictated by users; norms form around "free" logic, setting stage for ad-based models, content generated by users, and ambiguous data governance	Firm-level considerations of privacy and data governance emerge due to recognition of data as key organizational asset in new business models; institutional divergence in national approaches to data governance between US and other countries as US attempts to jockey for advantage in the emergent transnational field where fixed rules and dominant players are yet to be determined	Privacy concerns of users generate wide debate about data governance/ownership issues; firms are held to higher standards related to data use policies; users begin to take back control of their data with new practices and technologies, effectively blocking firms' unauthorized use of data

bubble burst in 2000. Discussions of governance were more focused on the Internet and cyberspace, as opposed to data, as these early years were characterized by a hands-off approach and adherence to a laissez-faire economic paradigm (Deibert & Rohozinski, 2010a, 2010b), which could be created and governed (or non-governed) by its users (Barrett & Strongman, 2012), with ambiguous or non-existent boundaries between users and producers. Although discussions in civil society may have been brewing at this time, personal data governance played second fiddle to more technical aspects of the Internet. Any norms that did emerge during the era of Web 1.0 were determined more organically via the collective activity and interactions of its users (Barrett & Strongman, 2012). Before the mid-1990s, the Internet was typified by a non-commercial logic, and free became the online norm. When commercial services emerged, the "free" logic was already firmly entrenched, and it became clear that advertising was the only available revenue model (Schneier, 2015).

This "free" logic ultimately led to the emergence of business models built around the use of individuals' data for advertising purposes as opposed to fee-based models, setting the stage for future issues surrounding the legitimate ownership of and authority to use individuals' data. It also set the stage for the legitimacy of a model where content was created by users themselves, with the firm's primary purpose as a platform and aggregator and seller of users' data.

Stage 2: Regulatory versus Normative Approaches to Personal Data Governance. In Stage 2, firm-level considerations of privacy and data governance began to emerge due to a growing recognition that personal data were a key organizational asset in many of the new technology companies starting up in this era. With personal data as an important asset, questions arose of how the individuals whose data were being used related to the firms using their data, and how (and whether) these individuals should be compensated, or at least informed, of the uses of their data. Issues and debates surrounding regulatory activities around informational privacy began to emerge, and a major division in information privacy legislation appeared between the approaches taken between the US and the EU. While the EU has taken a more regulatory approach, the US has relied more on normative pressures to govern information privacy, highlighting the fundamental differences between two divergent ideologies (Stahl, 2007) of privacy and data protection, with fundamental differences in *kind* rather than just in *degree* becoming apparent throughout the recent history of data governance in the respective jurisdictions (Smith, 2001). The European approach considered privacy to be a fundamental human right to be guarded through regulatory mechanisms, whereas the US approach entrusted the protection of personal privacy to the free market, and was wary of the intrusion on personal freedoms from the state over activities from market actors (Long & Quek, 2002).

In the US, the Federal Trade Commission (FTC) has had a particularly key role in shaping the normative approach to data governance in the US (Solove & Hartzog, 2014). In 1995, the FTC began to receive pressure from the US Congress to become involved with consumer privacy issues, particularly as it related to personal data and the Internet. The FTC undertook a self-regulatory model, whereby companies would create rules, and the FTC would provide legitimacy by overseeing and enforcing them (Solove & Hartzog, 2014). The FTC's primary source of authority is a section of their mandate that prohibits "unfair or deceptive acts or practices in or affecting commerce," and these two doctrines, unfairness and deception, have come to shape the FTC's approach with the data governance of DBBs' activities (Beltramini, 2003), which corresponds to the widely adopted norms of "notice and choice" discussed above.

Indeed, the FTC has made normative headway, codifying certain norms and best practices (Solove & Hartzog, 2014). Early attempts to use privacy torts or apply existing statutory law to address privacy concerns in online data gathering practices largely failed, leading to the FTC's current role as the main governing force for personal data privacy in the US. Despite the increasing number of privacy-related complaints (the annual number of complaints dealt with by the FTC increased three-fold in the decade between 2002 and 2012), few judicial changes have been made with nearly all cases ending in settlement agreements (Solove & Hartzog, 2014). These data governance issues are partially attributed to the sector-specific nature of personal data regulation in the US. Whereas many other industrial nations have a single set of laws that protects all personal data, the US has different laws that regulate different industries and economic sectors, leaving large areas, such as issues related to data collection by companies such as Facebook and Google, largely unregulated at the federal level (Solove & Hartzog, 2014).

The EU, on the other hand, has taken a stronger regulatory approach than the US. Beginning around the same time as the US' more firm-driven approach, the European Commission's 1998 Data Protection Directive is widely seen as the first major event related to European data protection law, and one which has been highly influential in shaping numerous laws both within the EU and elsewhere (Schwartz, 2013). This Directive prohibits the use of personal data of European citizens without the consent of the individual and his or her national government, requires companies to allow individuals access to their data, withholds personal data from unauthorized uses, and facilitates legal recourse (Long & Quek, 2002). The Directive also limits international data transfers to countries without "adequate" legal protections for personal information. While many countries in other regions, such as Canada and Australia, adopted new data privacy laws to harmonize their data protection standards to this benchmark, the US did not (Long & Quek, 2002). At the time of passage, the US did not meet this standard, and this lack of harmonization highlighted the clash between the US and EU's data protection policies, as well as the magnitude of the issue at hand, given that at the time the US and EU shared the largest trade and investment relationship in the world (Long & Quek, 2002). Motivated by technological advances facilitating increasing quantities of personal data being collected more innocuously, the European Commission is taking an increasingly strong stance in the protection of individuals' data, as evidenced by its release in January 2012 of a "General Data Protection Regulation," marking an important governance shift from directives to regulations (Schwartz, 2013).

These divergent approach between the US and EU to data governance highlight not only the transnational nature of data governance, given that data do not reside in any particular location, but also how these vastly different approaches within one transnational field suggests that as this field is emerging, that actors (albeit at the national level) are jockeying for advantage as rules and positions and power dynamics are as yet to be determined (Buchholz, 2016).[2]

Stage 3: Cognitive and Individual Approaches to Personal Data Governance. In stage 3, despite both normative and regulatory attempts to provide a safe and productive framework for data governance, in practice, it has become increasingly recognized that governance practices related to anonymity and consent have remained ineffectual or opaque (Barocas & Nissenbaum, 2014). The result is a recent shift towards a more individualized and user-oriented approach to data governance. Trends in scholarly debate diverge across three broad avenues. Although each takes as its starting point flaws in the current system, the first avenue seeks to identify how firms can alter perceptions of end users, or data subjects, about issues related to trust of online services, such as through "security signals" (privacy policies, perceived website investment, and reputation) (Ray, Ow, & Kim, 2011) or changes in privacy notices such as readability and length modifications (Milne, Culnan, & Greene, 2006). Milne et al. (2006) paradoxically found that privacy notices have grown in length and declined in readability, likely due to an increase in legal requirements for consent, ultimately leading to a decrease in actual consent, or "consent desensitization" (Schermer, Custers, & van der Hof, 2014).

A second stream debates the relative merits of stronger regulation over "privacy self-management," which provides individual control over personal data, facilitating individuals to weigh the costs and benefits of the collection, use, or disclosure of their information, and avoiding a regulatory approach that sidesteps consent all together (Solove, 2013). A third stream discusses a form of data governance that, although undertaken at the individual level, in substance is more akin to a social movement, also referred to as "digital direct action" (Coleman, 2013). While including leaks, hacking, and mass online protests at the more radical end of the spectrum, this is part of a larger movement of individuals who seek to take issues such as data privacy into their own hands, such as the practice of data obfuscation. Brunton and Nissenbaum (2012) describe data obfuscation as:

> … the production of misleading, ambiguous and plausible but confusing information as an act of concealment or evasion … a method that acts as informational resistance, disobedience, protest or even covert sabotage – a form of redress in the absence of any other protection and defence, and one which disproportionately aids the weak against the strong. (p. 1)

One example of this is the Firefox extension TrackMeNot. TrackMeNot is a free Firefox Browser extension that hides user search preferences, thereby avoiding the profiling of users through their searches, and stymieing targeted advertising attempts (Howe & Nissenbaum, 2009). This obfuscation-enabling technology was developed as the direct result of a disruptive event in 2006, when AOL disclosed the search queries of 650,000 of its users, illustrating how search logs, even anonymized logs, could be analyzed subsequently to reveal the identities of search engine users (Toubiana, Subramanian, & Nissenbaum, 2011). A less radical variety of privacy enhancing technology in this more individualized form of data privacy is encryption, which can be used for e-mail, web browsing, and hard drive blocking (Schneier, 2015).

DISCUSSION AND CONCLUSIONS

Despite the importance of the phenomenon of DBBs to the field of management, with a few notable exceptions (see e.g., Dutta & McCrohan, 2002; Pollach, 2005; Ray et al., 2011; Sarathy & Robertson, 2003; Smith, 2001), management scholars have yet to fully address this important topic (George, Haas, & Pentland, 2014). According to George et al. (2014),

> Though "big data" has now become commonplace as a business term, there is very little published management scholarship that tackles the challenges of using such tools—or, better yet, that explores the promise and opportunities for new theories and practices that big data might bring about. (p. 1)

Yet, other scholarly fields have followed this phenomenon with keen interest, and in the above review, I draw from a wide range of scholarly perspectives to delineate the phenomenon of the DBB, and trace the organizational field that has emerged around issues related to the governance of data in this industry, and the institutions that have formed around it in the various stages of its existence, through a series of field-configuring events, and by various actors. I argue that this phenomenon is of critical importance to organizational and management scholars, because of the questions it raises about appropriate organizational boundaries, the novel governance configurations that the field-level norms have created, and the implications for society. More specifically, this phenomenon has theoretical implications related to how the institutional field has emerged, and how it has affected the boundary permeability of organizational actors in the field. Additionally, it has implications related to discussions of organizational boundaries, such as those of interest to scholars of TCE; as well as how these unique boundary configurations affect society more broadly.

From the perspective of the institutional field, three key features of this phenomenon highlight its theoretical import. First, this is an example of an *emergent* issue field, providing an opportunity to trace how the development of this institutional field shapes the permeability of organizational boundaries through field-configuring events, the prioritization of actors, and the prioritization of the issues themselves. The institutional history of this emerging field demonstrates how, particularly in the US context, the boundaries of the field and its governance have been shaped only partially by regulatory bodies, but perhaps more significantly by individuals, whose overlapping roles as developers and users of the technologies significantly shaped the early non-commercial logic that set the stage for DBBs' later reliance on data as a primary revenue source. Paradoxically, it may be the very same "free" and democratic logic, initially designed to *protect* individual freedoms, that now underpins an approach to data governance that may actually *undermine* individuals' data freedoms by providing large corporations the ability to use the provision of "free" services as justification for a substantive loss of individual data privacy and control, without providing individuals a clear understanding of the full implications of this trade-off.[3] Second, this is an example of an *interstitial* issue field (Zietsma et al., 2016), which by nature has porous field boundaries, with members of various fields bringing disparate and often conflicting logics to bear on how the field and governance dynamics unfold amidst weak or non-existent institutional infrastructure (Hinings et al., 2017; Zietsma et al., 2016). The institutional history also highlights shifts in logics over time, from an initially free and democratic logic, to a commercial logic, to a more regulated logic, to a more individualized logic, as described in the institutional history of the DBB field. In addition, tracing this institutional history and the settlement on a "freemium" logic, requiring the use of individual data to form the backbone of the economic exchange, highlights an "institutional holdover" that was retained from the early stages of field emergence. More specifically, the early stages of this field emphasized the individual (as opposed to the organization), as well as the free and democratic use of web-based platforms as a central component to the emergent institutional infrastructure. As the field emerged and became increasingly commercialized and exchange-based, the individual and democratic aspects of the field's logic dissipated, yet the assumption that Internet-based services should be free had been imprinted from the early days, and this holdover precipitated that economic actors had to find other models to facilitate economic exchange.

Third, this is a *transnational* issue field, adding a further layer of institutional complexity, in light of the need to harmonize across policy borders. A comparative institutions lens may also provide future research avenues around the dynamics of harmonization of responses across borders, in light of distinct differences in logics (e.g., a human rights versus a property rights logic of data governance) and how they are reconciled across national borders. By tracing the divergent institutional paths of these national actors as they compete to see which set of institutional norms will become dominant as the institutional infrastructure solidifies, their effects on organizational boundaries are highlighted: within the subfield of the EU (and other countries who have harmonized with this approach), with its more regulatory approach to data governance, the responsibilities associated with safeguarding and use of data fall squarely within the boundaries of DBB firms, and accountability and enforcement mechanisms are in place to support this. Comparatively, within the subfield of the US, a more normative approach allows the responsibilities associated with data governance to rest more heavily on individuals to be mindful of each firms' individual and ever-changing data use and privacy policies.

This phenomenon is also theoretically generative from the perspective of organizational boundary porosity. As TCE and organizational boundary scholars seek to answer questions around how firms capture value at the transaction level of analysis, the phenomenon also surfaces important theoretical issues with regard to firm-level boundaries. When firms rely on business models that derive value from individuals' data, firm boundaries are necessarily more porous and it is increasingly unclear who the members of an organization are. This new model, and the uncertainty and complexity of data ownership that it creates, raises important questions around firm-level transactional governance, as it is unclear whether these important assets reside within or outside of the organization. Therefore, a transaction cost lens raises important questions around how these business models create, capture, and distribute value, when the value-generating asset is arguably located outside of the firm's boundaries, and when the transaction whereby value is exchanged is governed by tenuous claims that all transaction partners are clear on the nature of the transaction. When considering "value" as the sum of benefits obtainable from a given exchange (Kivleniece & Quelin, 2012), questions of data rights and ownership lead into theoretically interesting terrain of the value of data, at the individual, firm and societal level, and how the benefits are appropriated, both equitably and efficiently, and the governance configurations that may cause variation in this appropriation. Similar to the subprime mortgage lenders described by Mahoney, McGahan, and Pitelis (2009), which, the authors argued, engaged in excessive risk taking at the public's expense, DBB models are often opaque intermediaries who have little incentive to address the negative externalities their activities may produce. The governance structures that may dissuade these moral hazard incentives provide an important avenue of research, particularly in light of emergent views of property rights related to personal data (Victor, 2013).

Finally, this phenomenon sheds light on the boundaries of practices that can span from legitimate to illegitimate, without a clear line that divides the two ends of the continuum. In other words, this is an example of an issue that has ambiguous legitimacy boundaries, as the practice itself (i.e., the sale of individuals' data to advertising agencies or intermediaries) is legitimate, but extreme forms of the practice may become illegitimate, even as it may not be illegal, due to the governance gaps that characterize the field. Governance mechanisms may not exist to curtail the shift from legitimate practice to illegitimate exploitation, as the boundaries between legitimate and illegitimate are as yet unclear (Crawford & Schultz, 2014). Therefore, the permeability of organizational boundaries, and the field that has helped to shape it, has significant implications for society, particularly as it relates to questions of power. For example, the issue field described above also foregrounds the shifting nature of power dynamics brought about by data and those who have access to the insights it unlocks. In the "digital era," power is not absent, as it had initially been conceived, but "its exercise becomes more subtle and unobtrusive" (Powell et al., 2016, p. 10). Those organizations who may be most likely to cross the boundaries between legitimate and illegitimate uses of data may increasingly be the same organizations who shape what we see, in some cases based on who we are (Gandy, 1993). This new power structure simultaneously creates a large institutional field with regard to who is affected by it, but a miniscule subset that holds the power over it. As just one example of the tremendous power afforded to organizations that control the "data reins," consider Google's recent involvement in the payday lending industry, which many categorize as an industry with primarily negative societal implications. Some have credited the rise of payday lending with online payday lenders' ability to track and target impoverished individuals based on search terms such as "need to pay rent." As described by a statement by the Georgetown Law Center on Privacy and Technology, "You go to a search engine when you need help, when you're in trouble, broke, and you reveal to a search engine what you'd never reveal to anyone else" (Bowles & Jackson, 2016). In May of 2016, Google announced a ban on payday lenders offering loans at an annual percentage rate of 36 percent or higher from using Google's search platform. This was a major blow for the industry, and many of the industry's leading analysts speculated that "Google's decision could have as much or even more impact on curtailing the industry than any new regulation" (CBC, May 12, 2016). This raises questions about whether digital data (and those who control it) is becoming a new form of institutional force, perhaps even more potent than regulation.

The topic is also critical for a wide range of practitioners, including such diverse actors as managers, medical professionals, and policy makers, who must be increasingly aware of and sensitive to the ownership and ethics of information and data and related privacy issues in their daily decisions, and where the boundaries between legitimate and illegitimate lie. Practical considerations, such as the tradeoffs between using technology to monitor productivity and respecting employees' privacy, providing benefits to an increasingly distributed and freelance-based workforce, and weighing the allure of selling supporters' data as a revenue generating model for social enterprises against privacy considerations, are important ones that future organizational research studying this phenomenon will be well-positioned to answer.

In conclusion, this phenomenon provides an opportunity to extend extant theorizing related to the interplay of organizational boundaries and the institutional fields, and to explore the extent to which the porosity or permeability of organizational boundaries is determined by the characteristics and emergence of an institutional field. Providing definitional clarity and boundary conditions around an emerging yet opaque and under-studied (yet theoretically generative) phenomenon, as well as demonstrating its importance to questions of relevance to organizational scholars, will hopefully provide a foundation for future academic inquiry, and enhance theoretical understanding of organizational boundaries in light of novel organizational forms and models.

NOTES

1. Tracking is the capture of online behavior and information, which then feeds into the targeting of ads selected by analysis of the tracked data (Barocas & Nissenbaum, 2009).
2. With thanks to an editor of this volume for this observation.
3. With thanks to an editor of this volume for this observation.

REFERENCES

Acquier, A., Daudigeos, T., & Pinske, J. (2017). Promises and paradoxes of the sharing economy: An organizing framework. *Technological Forecasting and Social Change*, *125* (1), 1–10.

Afuah, A. (2003). Redefining firm boundaries in the face of the internet: Are firms really shrinking? *Academy of Management Review*, *28*(1), 34–53.

Ahrne, G., & Brunsson, N. (2008). *Meta-organizations*. Cheltenham: Edward Elgar Publishing.

Ahrne, G., & Brunsson, N. (2011). Organization outside organizations: The significance of partial organization. *Organization*, *18*(1), 83–104.

Anand, N., & Watson, M. R. (2004). Tournament rituals in the evolution of fields: The case of the grammy awards. *The Academy of Management Journal*, *47*(1), 59–80.

Andrejevic, M. (2014). Big data, big questions| the big data divide. *International Journal of Communication*, *8*(1), 1673–1689.

Barocas, S., & Nissenbaum, H. (2009). *On notice: The trouble with notice and consent*. In Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information. Retrieved from https://ssrn.com/abstract=2567409

Barocas, S., & Nissenbaum, H. (2014). Big data's end run. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy big data, and the public good: Frameworks for engagement* (pp. 44–75). Cambridge: Cambridge University Press.

Barrett, J., & Strongman, L. (2012). The Internet, the law, and privacy in New Zealand: Dignity with liberty. *International Journal of Communication*, *6*, 127–143.

Belk, R. (2014). You are what you can access: Sharing and collaborative consumption online. *Journal of Business Research*, *67*(8), 1595–1600.

Beltramini, R. F. (2003). Application of the unfairness doctrine to marketing communications on the internet. *Journal of Business Ethics*, *42*(4), 393–400.

Botsman, R. (2013). The sharing economy lacks a shared definition. *Fast Company*, 21. Retrieved from https://www.fastcompany.com/3022028/the-sharing-economy-lacks-a-shared-definition

Bowles, N., & Jackson, J. (2016, 11 May). 'Dangerous' payday loans join guns and drugs on Google's banned ad list. *The Guardian*.

Boyd, D., & Crawford, K. (2012). Critical questions for big data. *Information, Communication & Society*, *15*(5), 662–679.

Briscoe, F., Gupta, A., & Anner, M. S. (2015). Social activism and practice diffusion: How activist tactics affect non-targeted organizations. *Administrative Science Quarterly*, *60*(2), 300–332.

Brunton, F., & Nissenbaum, H. (2011). Vernacular resistance to data collection and analysis: A political theory of obfuscation. *First Monday*, *16*(5), Retrieved from http://firstmonday.org/article/view/3493/2955

Brunton, F., & Nissenbaum, H. (2012). Political and ethical perspectives on data obfuscation. In M. Hildebrandt & K. de Vries (Eds.), *Privacy, due process and the computational turn* (pp. 171–195). Abingdon, Oxon: Taylor & Francis. doi:10.4324/9780203427644

Buchanan, S. (2016). *Trade associations and the strategic framing of change in contested issue organizational fields: The evolution of sustainability in the Canadian mining industry, 1993–2013*. Doctoral dissertation, York University.

Buchholz, L. (2016). What is a global field? Theorizing fields beyond the nation-state. *The Sociological Review Monographs*, *64* (1), 31–60.

Byrne, E. F. (1996). The two-tiered ethics of electronic data processing. *Philosophy and Technology*, *2*(1), Retrieved from http://scholar.lib.vt.edu/ejournals/SPT/v2_n1pdf/BYRNE.PDF

Coleman, G. (2013). Anonymous in context: The politics and power behind the mask. *CIGI Internet Governance Papers*, *3*(1), Retrieved from https://www.cigionline.org/sites/default/files/no3_8.pdf

Crane, A. (2010). From governance to governance: On blurring boundaries. *Journal of Business Ethics*, *94*, 17–19.

Crawford, K., & Schultz, J. (2014). Big data and due process: Toward a framework to redress predictive privacy harms. *Boston College Law Review*, *55*(1), 13–64.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115.

Denardis, L. (2013). Multi-stakeholderism: The internet governance challenge to democracy. *Harvard International Review*, *34*(4), 40.

Deibert, R., & Rohozinski, R. (2010a). Liberation vs. control: The future of cyberspace. *Journal of Democracy*, *21*(4), 43–57.

Deibert, R. J., & Rohozinski, R. (2010b). Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology*, *4*(1), 15–32.

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review*, *45*(1), 67–87.

Egels-Zandén, N., & Hyllman, P. (2006). Exploring the effects of union-ngo relationships on corporate responsibility: The case of the Swedish clean clothes campaign. *Journal of Business Ethics*, *64*(3), 303–316.

Gandy, O. H., Jr. (1993). *The panoptic sort: A political economy of personal information. Critical studies in communication and in the cultural industries*. Boulder, Colorado:Westview Press.

Gandy, O. J. (2005). *If it weren't for bad luck*. 14th Annual Walter and Lee Annenberg Distinguished Lecture. Retrieved from http://www.asc.upenn.edu/usr/ogandy/Annenberg%20Lecture.pdf

George, G., Haas, M. R., & Pentland, A. (2014). Big data and management. *Academy of Management Journal*, *57*(2), 321–326.

Greenwood, R., Hinings, C. R., & Whetten, D. (2014). Rethinking institutions and organizations. *Journal of Management Studies*, *51*(1), 1206–1220.

Greenwood, R., & Suddaby, R. (2006). Institutional entrepreneurship in mature fields: The big five accounting firms. *Academy of Management Journal*, *49*(1), 27–48.

Greenwood, R., Suddaby, R., & Hinings, C. R. (2002). Theorizing change: The role of professional associations in the transformation of institutionalized fields. *Academy of Management Journal*, *45*(1), 58–80.

Hardy, C., & Maguire, S. (2010). Discourse, field-configuring events, and change in organizations and institutional fields: Narratives of ddt and the stockholm convention. *Academy of Management Journal*, *53*(6),1365–1392.

Helms, W. S., Oliver, C., & Webb, K. (2012). Antecedents of settlement on a new institutional practice: Negotiation of the ISO 26000 standard on social responsibility. *Academy of Management Journal*, *55*(5), 1120–1145.

Hinings, C. R., Logue, D., & Zietsma, C. (2017). Fields, governance and institutional infrastructure. In. R. Greenwood, C. Oliver, T. B., Lawrence, & R. Meyer (Eds.), *SAGE handbook of organizational institutionalism* (pp. 163–189, 2nd ed.). London: SAGE.

Hoffman, A. J. (1999). Institutional evolution and change: Environmentalism and the U.S. chemical industry. *The Academy of Management Journal*, *42*(4), 351–371.

Hood, C. (2006). Transparency in historical perspective. In. C. Hood & D. Heald (Eds.), *Transparency: The key to better governance* (pp. 3–23). Oxford: Oxford University Press.

Howe, D. C., & Nissenbaum, H. (2009). TrackMeNot: Resisting surveillance in web search. *Lessons From the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*, *23*(1), 417–436.

Kivleniece, I., & Quelin, B. V. (2012). Creating and capturing value in public-private ties: A private actor's perspective. *Academy of Management Review*, *37*(2), 272–299.

Long, W. J., & Quek, M. P. (2002). Personal data privacy protection in an age of globalization: The US-EU safe harbor compromise. *Journal of European Public Policy*, *9*(3), 325–344.

Lyon, D., & Burton, J. R. (1995). The electronic eye: The rise of surveillance society. *Journal of Consumer Affairs*, *29*(2), 486–488.

Maguire, S., Hardy, C., & Lawrence, T. B. (2004). Institutional entrepreneurship in emerging fields: HIV/AIDS treatment advocacy in Canada. *Academy of Management Journal*, *47*(5), 657–679.

Mahoney, J. T., McGahan, A. M., & Pitelis, C. N. (2009). Perspective – The interdependence of private and public interests. *Organization Science*, *20*(6), 1034–1052.

Mayo, V. (May 12, 2016). *Google bans ads from payday lenders, calling them 'harmful'*. The Associated Press, CBC News.

Meyer, R. E., & Höllerer, M. A. (2010). Meaning structures in a contested issue field: A topographical map of shareholder value in Austria. *Academy of Management Journal*, *53*(6), 1241–1262.

Milne, G. R., Culnan, M. J., & Greene, H. (2006). A longitudinal assessment of online privacy notice readability. *Journal of Public Policy & Marketing*, *25*(2), 238–249.

Nafus, D., & Sherman, J. (2014). Big data, big questions| this one does not go up to 11: The quantified self movement as an alternative big data practice. *International Journal of Communication*, *8*, 1784–1794. Retrieved from http://ijoc.org/index.php/ijoc/article/view/2170/1157

Newman, A. L. (2010). What you want depends on what you know: Firm preferences in an information age. *Comparative Political Studies*, *43*(10), 1286–1312.

Nickerson, J. A., & Silverman, B. S. (2003). Why firms want to organize efficiently and what keeps them from doing so: Inappropriate governance, performance, and adaptation in a deregulated industry. *Administrative Science Quarterly*, *48*(3),433–465.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32–48.

Ocasio, W., & Radoynovska, N. (2016). Strategy and commitments to institutional logics: Organizational heterogeneity in business models and governance. *Strategic Organization*, *14*(4), 287–309.

Ozcan, P., & Eisenhardt, K. M. (2005). *New firms in an emergent market: Building a strong alliance portfolio from a low-power position*. Working paper, IESE.

Pentland, A. (2011). Personal data: The emergence of a new asset class. In. *World Economic Forum*. Retrieved from http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

Pfeffer, J., & Salancik, G. (1978). *The external control of organizations: A resource dependence perspective*. New York, NY: Harper & Row Publishers.

Pollach, I. (2005). A typology of communicative strategies in online privacy policies: Ethics, power and informed consent. *Journal of Business Ethics*, *62*(3), 221–235.

Poppo, L., & Zenger, T. (1998). Testing alternative theories of the firm: Transaction cost, knowledge-based, and measurement explanations for make-or-buy decisions in information services. *Strategic Management Journal*, *19*(9), 853–877.

Powell, W. W., Oberg, A., Korff, V. P., Oelberger, C., & Kloos, K. (2016). Institutional analysis in a digital era: Mechanisms and methods to understand emerging fields. In *New Themes in Institutional Analysis: Topics and Issues From European Research*. Cheltenham, UK: Edward Elgar.

Purdy, J. M., & Gray, B. (2009). Conflicting logics, mechanisms of diffusion, and multilevel dynamics in emerging institutional fields. *Academy of Management Journal*, *52*(2), 355−380.

Rao, H., Morrill, C., & Zald, M. N. (2000). Power plays: How social movements and collective action create new organizational forms. *Research in Organizational Behavior*, *22*(1), 237−281.

Ray, S., Ow, T., & Kim, S. S. (2011). Security assurance: How online service providers can influence security control perceptions and gain trust. *Decision Sciences*, *42*(2), 391−412.

Reidenberg, J. R. (2000). Resolving conflicting international data privacy rules in cyberspace. *Stanford Law Review*, *52*, 1315−1371.

Santos, F. M., & Eisenhardt, K. M. (2005a). *Constructing markets and organizing boundaries: Entrepreneurial action in nascent fields*. Working paper, INSEAD.

Santos, F. M., & Eisenhardt, K. M. (2005b). Organizational boundaries and theories of organization. *Organization Science*, *16*(5), 491−508.

Sarathy, R., & Robertson, C. J. (2003). Strategic and ethical considerations in managing digital privacy. *Journal of Business Ethics*, *46*(2), 111−126.

Scaraboto, D., & Fischer, E. (2013). Frustrated fatshionistas: An institutional theory perspective on consumer quests for greater choice in mainstream markets. *Journal of Consumer Research*, *39*(6), 1234−1257.

Schermer, B. W., Custers, B., & van der Hof, S. (2014). The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology*,*16*(2), 171−182.

Schneier, B. (2015). *Data and goliath: The hidden battles to collect your data and control your world*. New York, NY: W. W. Norton & Company.

Schüssler, E., Rüling, C.-C., & Wittneben, B. B. F. (2014). On melting summits: The limitations of field-configuring events as catalysts of change in transnational climate policy. *Academy of Management Journal*, *57*(1), 140−171.

Schwartz, P. M. (2004). Property, privacy, and personal data. *Harvard Law Review*, *117*(1), 2056−2128.

Schwartz, P. M. (2013). The EU-US privacy collision: A turn to institutions and procedures. *Harvard Law Review*, *126*(7), 1966−2009.

Schwarz, G., & Stensaker, I. (2014). Time to take off the theoretical straightjacket and (re-) introduce phenomenon-driven research. *The Journal of Applied Behavioral Science*, *50*(4), 478–501.

Scott, W. R. (1995). *Institutions and organizations* (Vol. 2). Thousand Oaks, CA: Sage.

Smith, H. J. (2001). Information privacy and marketing: What the US should (and shouldn't) learn from Europe. *California Management Review*, *43*(2), 8−33.

Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, *126*(7), 1880−1903.

Solove, D. J., & Hartzog, W. (2014). The FTC and the new common law of privacy. *Columbia Law Review*, *114* (1), 583−1033.

Stahl, B. C. (2007). Privacy and security as ideology. *Technology and Society Magazine, IEEE*, *26*(1), 35−45.

Toubiana, V., Subramanian, L., & Nissenbaum, H. (2011). Trackmenot: Enhancing the privacy of web search. ArXiv, 1109.4677(1). Retrieved from https://arxiv.org/pdf/1109.4677.pdf

Victor, J. M. (2013). The EU general data protection regulation: Toward a property regime for protecting data privacy. *The Yale Law Journal*, *123*(2), 513−551.

Williamson, O. E. (1975). *Markets and hierarchies: Analysis and antitrust implications*. New York: Free Press.

Williamson, O. E. (1981). The economics of organizations: The transaction cost approach. *American Journal of Sociology*, *87*(3), 548−577.

Zietsma, C., Groenewegen, P., Logue, D., & Hinings, C. R. (2016). Field or fields? Building the scaffolding for cumulation of research on institutional fields. *Academy of Management Annals*, *10*(1), 3–107.

Zietsma, C., & Lawrence, T. (2010). Institutional work in the transformation of an organizational field: The interplay of boundary work and practice work. *Administrative Science Quarterly*, *55*, 189–221.