Article

Business & Society
1–17

DOI: 10.1177/0007650317727540
journals.sagepub.com/home/bas

The Governance of Digital Technology, Big Data, and the Internet: New Roles and Responsibilities for Business

Mikkel Flyverbom[1], Ronald Deibert[2], and Dirk Matten[3]

Abstract

The importance of digital technologies for social and economic developments and a growing focus on data collection and privacy concerns have made the Internet a salient and visible issue in global politics. Recent developments have increased the awareness that the current approach of governments and business to the governance of the Internet and the adjacent technological spaces raises a host of ethical issues. The significance and challenges of the digital age have been further accentuated by a string of highly exposed cases of surveillance and a growing concern about issues of privacy and the power of this new industry. This special issue explores what some have referred to as the "Internet-industrial complex"—the intersections between business, states, and other actors in the shaping, development, and governance of the Internet.

Keywords

big data, data collection, governance, Internet, Internet-industrial complex, privacy

[1]Copenhagen Business School, Frederiksberg, Denmark
[2]University of Toronto, Onatrio, Canada
[3]York University, Toronto, Onatrio, Canada

Corresponding Author:
Mikkel Flyverbom, Department of Management, Society and Communication, Copenhagen Business School, Dalgas Have 15, DK-2000 Frederiksberg, Denmark.
Email: mf.msc@cbs.dk

New eras are often marked by events that live on in anecdotes. In 2012, an angry father turned up at a Target store in the United States challenging the manager as to why the company sent promotional material for products focusing on pregnant women to his 16-year-old daughter, at the time still in high school. It turned out that his daughter indeed had shopped at Target, and the company's data analytics had inferred from the products in her shopping basket that she must be pregnant. Hence, their algorithms figured out that targeting her with tailored advertising and coupons would be an efficient way of promoting their products. The irony of this case, of course, was that obviously Target "knew" well before the girl's father, that his daughter was pregnant—which indeed she was (Duhigg, 2012).

This anecdote drew the public's attention to three new features of an emergent phenomenon, which would quickly become known as "big data." First, companies gather comprehensive data about our life, either because we provide data in exchange for free services provided by Internet companies or are unaware of the forms and extents of data aggregation and brokering for commercial purposes at play in digital spaces. Second, new technologies in data processing have put companies in a position to analyze and combine vast amounts of information which provide knowledge about individuals beyond anybody's imagination. Third, the anecdote also exemplifies some of the ethical issues: such knowledge now in the hands of corporations allows them to encroach on privacy and affect individuals' lives at an unprecedented scale.

In broader terms, the importance of digital technologies for social and economic developments and a growing focus on data collection and privacy concerns have made the Internet a salient and visible issue in the public domain. Recent developments, such as the information released by Edward Snowden and others, have increased the awareness that the current approach of governments and corporations to the governance of the Internet and the adjacent technological spaces raise a host of ethical, political, legal, and rights-related issues. Examples include states tracking citizens online, governments filtering or turning off the Internet at will, and corporations using personal data for commercial purposes. The significance and challenges of digital transformations have been further accentuated by a string of highly exposed cases of surveillance and a growing concern about how states and corporations use digital traces to do various sorts of tracking and profiling of citizens and users. But surveillance and privacy concerns are only the most visible of a host of issues in need of attention. Despite the growing focus on digital transformations, surprisingly little research has explored questions about the relations between business, governance, and the Internet. This special issue of *Business & Society* explores what some have referred to as the "Internet-industrial complex"—the intersections between business, states, and other actors in the shaping, development and governance of the Internet.

Digital Transformations

Digital technologies are increasingly central to people, corporations, and societies. Searching for information, staying in touch with friends and families, and navigating the city are just the most obvious examples of our growing dependency on digital technologies. Digital transformations also shape work processes by automating activities, and create new possibilities for organizations to rethink and optimize what they do, that is to "informate" (Zuboff, 1988). In everyday and organizational settings, digital technologies create new kinds of visibilities, better possibilities for editing, increased persistence of information, and more extensive forms of association (Treem & Leonardi, 2012). In the past, we used to think of digital technologies as tools that corporations and other organizations would pick up and use for particular activities. But increasingly, they are the backbone of most organizational processes and much of what we know about people, organizations, and societies involves digital sources and activities. This central and infrastructural role requires that we give more attention to the configurations, workings, and consequences of digital transformations.

A short history of these developments and their ramifications highlights that as different technologies evolve and converge, they create particular ecosystems, become tied to societal expectations, and condition certain forms of use. At present, these digital transformations take two primary shapes: what we can think of as digitalization and datafication.

Digitalization

The progression from analog to digital operations was a long and slow process, and even if digital technologies were available, they were often difficult to use. Just consider the first hard disks developed in the 1950s. Weighing over a ton and so bulky that they required a forklift to be transported, these were able to store 5MBs of data—about the size of a Beyoncé song in decent quality. Despite not being immediately useful, such technological developments laid the foundation for the automation and digitalization of a wide range of corporate and societal phenomena, such as keeping track of inventories, accounts, and populations. Paper files and other objects could be turned into digital bytes and copied, stored, and circulated in new ways and with much greater ease. Commercial and other financial transactions could be carried out via digital systems, and advertising and public relations activities found new channels and formats. With the development and spread of the Internet, advances in digitalization gained traction and became central to many parts of social life. These possibilities continue to have wide-reaching consequences for commercial and organizational activities, and they have

fundamentally transformed production processes, the management of information, and demands for human resources and capacities. As a result, phenomena such as outsourcing, the deterritorialization of production and the emergence of virtual, amorphous value chains became possible and advantageous. In particular, digital platforms, chips and bar codes, and other forms of monitoring and managing production flows have been central to the digitalization of commerce and enterprise. But despite these digital transformations, information remained a sparse and costly resource, and the extraction of actionable insights remained complicated and labor-intensive.

Datafication

Facilitated by these processes of digitalization, a second kind of digital transformation has emerged in more recent years. Many Internet companies started out with quite specific orientations and business models, but have realized that the data generated by interactions, user-generated content, and a wealth of other digital activities are potentially valuable resources (see West, 2017). These uses of the digital traces we all leave when navigating in digital spaces are central to the development of digitalization into what we can think of as "datafication" (Mayer-Schönberger & Cukier, 2013). By datafication we mean both the masses of digital traces left by people and technologies in online spaces and the proliferation of advanced tools for the integration, analysis, and visualization of data patterns for purposes of decision making and commercialization. Datafication implies that many parts of social life take the shape of digital traces. Friendships become "likes" on Facebook, movements through the city produce extensive digital footprints in GPS-enabled devices, and our searches for information show what we value or wish for as individuals and societies. An extraordinary volume of additional data is transmitted unconsciously and largely invisibly (to most users) simply as a result of Internet-connected devices communicating with each other once they are powered up. In between the two is metadata—literally, data about data—such as the routing information contained in the headers of emails or text messages, or geolocation information hidden within a digital photograph. As structured information, metadata can be more readily compared and analyzed by algorithms, and thus can often yield extraordinarily precise details about peoples' interests, movements, and relationships. Therefore, Internet companies providing platforms for such activities have access to mind-blowing amounts of data about everything we do, care about, and search for. Combined with automated sorting mechanisms, such as algorithms and artificial intelligence, these massive streams of digital traces can be used to show important patterns and inform a growing number of decisions about consumers, diseases, or criminal

activities. The realization that digital traces have value means that many Internet companies and digital platforms seek to both lock in users early on—to become the place where people buy books or stream movies, for instance—and to build closed off ecosystems or "walled gardens" where they can control and extract value from data. These developments are central to emergent concerns about the corporate centralization of what was intended to be a decentralized, distributed network of networks, as well as antitrust lawsuits stressing the problematic emergence of monopolies in the digital realm.

The Consequences of Digital Transformations

Internet companies constitute a relatively new industry, and one which plays a number of societal roles in need of our attention. They not only provide (often free) services, such as platforms for communication, information searches, or social connections, but also shape other industries and come to reconfigure established institutions. Advertising increasingly relies on the services of digital platforms, hotels have to compete with Airbnb, taxi drivers desperately seek to fend off Uber, and the business models of newspapers and publishing houses crumble as people drop their subscriptions, read via social media and companies advertise elsewhere. With access to more data and better abilities to turn them into value, digital platforms can target a wide range of other industries, such as when data about cities generated as a by-product by Uber drivers allows the company to crush established map producers because it has better, fine-grained and real-time data. But as these techniques and possibilities develop, they also travel into other domains, such as intelligence gathering, policing, and illicit forms of tracking and profiling. One example is applications and plug-ins that get instant access to a wide range of user data contained in electronic devices, from contacts, to archives of text messages, to images and videos as well as geolocation. These blanket permissions (sometimes even without users' consent) suck up not only individuals' social media profiles, but also those of all their contacts and friends. These valuable types of data travel quickly and widely in the new digital ecosystems provided by Internet companies such as Facebook, Google, Snapchat, and Twitter, but also often leak into, or otherwise end up in the hands of criminal associations, government agencies, or others. When thinking about the shape and significance of digital transformations, we need to consider such different dimensions as the size and dominance of Internet giants, the disruption of markets and industries, the nature of new acquisitions and monopolies, questions about U.S. dominance and standards, the extensive alliances between corporations and states, and the ramifications of widespread forms of surveillance and tracking. But we also need to give attention to the largely invisible ways in which digital

spaces structure information and guide our attention. This type of influence is an overlooked, but significant dimension of processes of digitalization and datafication: Internet companies and digital platforms shape our views of the world by managing, editing, and controlling information in ways that have important consequences for individuals, organizations, and societies alike (Flyverbom, 2016).

In combination, processes of digitalization and datafication create novel conditions for corporate activities, societal governance, and fundamental issues such as how we understand and view the world around us. These conditions require that we consider questions such as how we perceive and treat digital data, and how these digital transformations become entangled with societal developments, such as new forms of capitalism, new modes of production, the editing of social realities, and emergent forms of governance.

Relevance to the Business and Society Debate

The academic debate in the business and society field has so far given the topic and phenomenon of information technology (IT) and big data industry relatively short shrift. If anything, the reception and the potential benefits have been seen in a rather positive light, enhancing and encouraging the role of business in society in general (Tapscott & Ticoll, 2003). Specific areas have been discussed on the pages of this journal, for instance, in the environmental performance of business where new IT solutions have considerable potential (e.g., Carberry, Bharati, Levy, & Chaudhury, 2017), or the generation of new forms of corporate legitimacy through social media (Etter, Colleoni, Illia, Meggiorin, & D'Eugenio, 2017). Another example is the rise of sharing platforms, and generally what is now referred to as the "sharing economy" which in terms of more efficient resource use has been perceived as a substantial contribution to a more sustainable future (Cohen & Kietzmann, 2014). This uncritical attention in some ways also reflects the relative low level of public scrutiny many IT companies have received. For example, while apparel companies such as GAP or Nike have faced strong criticism about the labor conditions in their supply chains since the 1990s, a company such as Apple only since 2012 has been exposed to accountability demands for the labor conditions at their key Chinese supplier Foxconn (Duhigg & Barboza, 2012). Only rather recently many of the problematic aspects of corporate social responsibility (CSR) of the big data industry have entered the debate, and then conspicuously not in the classic journals of the business and society field (Martin, 2015; Richards & King, 2014; Zwitter, 2014).

Part of the reason might be the structure of the industry. After all, many of these companies are rather young and initially small and have displayed their

enormous growth only in the past two decades. Until very recently, only very few of them had the very size and brand recognition which typically has put companies and industries under public scrutiny. An additional momentum has also been that in many instances, Google or Facebook perhaps being the most well-known examples, the services have been, and are still in many instances, offered to users for "free."

Another more substantial reason lies in fact in the very structure and working mechanisms of the industry. The emergence of the digital economy has given rise to the phenomenon of "platform businesses" whose value creation consist mostly in offering products, services, or technologies that provide the foundation upon which outside firms (organized as a "business ecosystem") can develop their own complementary products, technologies, or services (Gawer & Cusumano, 2014; Wareham, Fox, & Cano Giner, 2014). The boundaries of these organizations are fuzzy and they differ markedly from traditional (analog) business models. Companies such as Uber, Airbnb, or Shopify create value more as a hub of a broader network for other players rather than as an alone standing and operating organizational unit. Furthermore, such changes in business models and patterns of value creation then are also manifest in a new role of "consumers." In fact, if users employ the services of these companies they end up, rather than being consumers, being more like producers in that one of those companies' crucial resource is the data collected from the users (Schneier, 2015). Internet companies seem to be expanding and operating in ways that differ markedly from more established and recognizable forms of business, and we still need to articulate the forms of value creation, enterprise and capitalism they are building (West, 2017; Zuboff, in press).

From the perspective of business responsibilities, this raises a number of questions which transcend the usual impacts of business on society—some of which we will discuss further down. The key new question about business responsibility arises from these new forms of business models, and how they are governed. While there is a rich literature in the business and society field on self-regulation and self-governance of organizations, industries, and sectors (Dashwood, 2014; Vogel, 2010), rather scant attention has been paid to the IT and big data sector in the management literature. In this special issue, then, we attempt at filling this gap and opening the debate to consider the longer standing discussions in neighboring social science disciplines.

Governing the Internet

Over the last several decades, as the Internet and associated technologies have deeply permeated all of society and have become critical to the

functioning of everyday life, governments have been drawn increasingly into Internet governance matters, ranging from economic to national security considerations. Whereas at one time only a few decades ago, few governments had Internet policies to speak of, today governance of the digital domain is among the most cross-cutting and important, with the security of cyberspace ranked as among the most pressing. Internet governance is further complicated by the fact that the domain involves multiple stakeholders, including businesses, government agencies, and civil society. Decisions taken by each of these stakeholders on their own can have potential system-wide effects and each of these stakeholders' preferences must be factored into Internet governance issues. For example, because the bulk of what we call the Internet is in the hands of the private sector, governments are compelled to enlist, coerce, or otherwise compel companies in their formal governance efforts. Private companies must be responsive to the laws of the countries within which they offer services. These laws can vary widely and have bearing on many aspects of the services, ranging from content takedown to the handling, retaining, and sharing of user data to censorship and surveillance. It is now routine for governments to impose regulations on Internet service companies in exchange for operating in their jurisdictions. Some of these regulations can be quite complex and intrusive, and shrouded in secrecy. For example, China requires by law all companies operating in its jurisdiction to police their networks, and to share user data with authorities upon notice. Research carried out at the Citizen Lab at University of Toronto has found that many popular China-based mobile applications used for instant messaging and live-streaming contain hidden censorship and surveillance functionalities presumably because of these requirements.

Meanwhile, private sector entities that control the services and the infrastructure are engaged in a type of governance as a result of their business and operating decisions quite apart from government regulations. Facebook, Google, Twitter, and other companies using sophisticated algorithms to control advertisements and news feeds can shape what billions of users read, share, purchase, and communicate—what West (2017) terms "data capitalism." Social media companies are not necessarily required to protect speech in the same way that governments are required to do (e.g., the U.S. First Amendment), because they are private platforms. They are more akin to shopping malls than public squares in this respect. The decisions they make have the effect of political consequences. These pressures and expectations on the private sector have brought about concerns around CSR, the Internet, and big data. While CSR concerns are relatively mature in other areas, they are still relatively new to the digital world (a topic examined in more detail below).

Internet governance is also characterized by a unique convergence of national security and information business interests around information gathering and data analysis—around mass and targeted surveillance. For states, the threat environment has shifted over the last few decades. Whereas for most of modern history the primary security concern of most states was the threat posed by other states, today the primary threat is dispersed across all of society, inside and outside of states. This new threat environment means that the "gaze" of state defense and intelligence agencies has become omnidirectional, anticipating threats in all directions, at all times. On the part of businesses, the economic engine at the heart of the cyberspace revolution is the commodification of personal information—likes, habits, movements, relationships—acquired through mass data acquisition of users' communications by companies such as Google and Facebook. In between the two engines of mass surveillance is a multibillion dollar data analysis, exploitation, and prediction economy that services both governments and companies. This convergence of interests is where "Big Brother" meets "Big Data," creating a powerful and very difficult-to-reverse set of social forces around the expansion of mass surveillance and commodification of personal information.

There is also Internet governance that takes place at the infrastructure layers, involving how technological systems operate and peer with each other. Most of these decisions are the result of standards developed by a community of peers, typically engineers and computer scientists propagated among themselves or through regional and international standard-setting bodies. Occasionally, the decisions taken at these forums can be influenced by governments, acting alone or in concert. For example, two standards organizations, the Alliance for Telecommunications Industry Solutions (ATIS) and the European Telecommunications Standards Institute (ETSI) primarily help define how global telecommunications companies collect, retain, and share the data traversing through their services networks to comply with lawful access requests from governments. The deliberations of these organizations include businesses, government agencies (primarily law enforcement), and some civil society.

As the Internet is global in scope, its governance is inherently an international problem even though there is no one single forum or regime of Internet governance. Instead, discussions around the norms, principles, and rules of the Internet are spread across multiple regional and international forums, from the International Telecommunications Union to the Internet Governance Forum to the standards setting bodies mentioned above. Although it would be simplistic to suggest a simple-dualism, there has been a general tension in recent years between two camps: those governments that prefer a less centralized governance regime with multistakeholder participation versus those, led

by China and Russia, that advocate for a more top-down, state-directed model. The 2013 disclosures by former National Security Agency (NSA) contractor Edward Snowden complicated this debate, fueling concerns among many policymakers that the Internet was a tool of U.S. control that required correction in the form of some kind of "technological sovereignty" which lends itself to the top-down, state-directed model (Deibert, 2015).

Responsible Business and Digital Transformations—Issues and Contentions

The area of digital technologies, the Internet, and the ascending big data industry offers a rich field of study from the perspective of responsible business inquiry. To begin with, and as an upshot, there are numerous societal benefits and contributions to the public good which we can identify as outcomes and effects, some of which even address longstanding ethical concerns around the role of business in society (Martin, 2015). Those contributions to the public good can range over a large number of areas. Be it contributions to public safety, law enforcement, and crime prevention, over to improvements in health care, education, or urban planning—in many of these areas this new industry has made a significant contribution. But also in terms of consumer benefits—be it the convenience and price reductions of online shopping, new transportation, housing services, or music consumption—this new industry has transformed many areas of life in an arguably beneficial way. In particular, the availability of big data services on mobile devices has provided many goods and services to the so-called developing world and has enabled access to hitherto unavailable goods and services in areas which, for a long time, were shunned by large corporations (Runhaar & Lafferty, 2009). Other commentators have stressed the benefits of these technologies in wider areas of public and political life, in that these technologies enable new forms of citizen's participation in the political process, leading some commentators even to talk about phenomena such as "Democracy 2.0" (Tapscott, 1997).

While these contributions are undisputed, the public debate in recent years, though, has increasingly zoomed in on the potential risks and ethical challenges raised by the industry. We can outline these by following Martin's (2015) modeling of the big data industry along the data flow, or "supply chain": from upstream (i.e., data generation), over manufacturing (i.e., data processing and aggregation), to downstream (i.e., data usage).

The most common ethical issue at the upstream level is the issue of violation and intrusion of privacy, the consent of the data provider, and the transparency with which big data companies collect the information. While these issues have always been known as challenges to business responsibilities

(i.e., in the area of human resource management or market research), the new technologies developed over the last two decades have given this problem a widely new dimension (Howe & Nissenbaum, 2009; Sarathy & Robertson, 2003). This is by no means singularly an issue for the private sector: Governments—though often using technologies and platforms of private companies—have gained substantial opportunities for the surveillance of communications, movements, behavioral patterns, and political activities of citizens. This surveillance has been acknowledged for a while, in particular in the context of oppressive regimes, and many companies such as Yahoo, Microsoft, or Google have faced criticism for their alleged complicity, for instance, with the Chinese government (Tan & Tan, 2012). Ever since whistleblowers (Edward Snowden being the most prominent case) revealed similar practices being normality for most governments in liberal democracies, too, it is clear that these practices are by no means just a question of oppressive regimes. The interesting aspect in the context of this special issue then is that, often these activities by governments are carried out with technology and services directly provided by private corporations. The theme of this special issue is in many ways a further and more in-depth illustration of a growing entanglement of corporations in the governance of public and political processes, a subject of an earlier special issue on the pages of this journal (Scherer, Palazzo, & Matten, 2014).

The "manufacturing" stage can be considered as the main domain more or less singularly controlled by data brokers and Internet companies. Responsibility issues out of this very activity then pertain to the fact that even if data are gathered upstream with consent and transparency, the combination of them might provide new metainformation which does no longer live up to those criteria discussed earlier. It is here where consumer profiles or, even further, profiles of vast parts of individuals' (or citizens') lives can be generated. It is generally an issue of wide concern that the public—be it upstream as data source or downstream as data users—has little, if any, transparency of how big data companies operate and what exactly happens to personal data there.

But the industry, in this manufacturing stage, faces also a number of other issues in itself. Human relations management–related issues have been widespread concerns. While many of these companies generally are hailed for fairly innovative human resource practices and lavish benefits, the ethical issues around new job profiles have received scant attention. Examples are "data janitors" (who review offensive and unethical data posted by users) with often severe results on the long-term mental health of the workers. Another group of issues in the "sharing economy" arises from the fact that users of platforms such as Uber or Amazon are paid relatively low wages with no pension or benefits or any other of the usual protections in the workplace. The

debate about "mechanical turks" (workers who offer their services via Internet platforms) and in general the working conditions in the "gig economy" illustrate many of the contentions big data companies may face.

Looking at the wider industry structure, a growing issue seems to be—as both the articles by Whelan (2017) and by Chenou and Radu (2017) in this special issue illustrate—that the platform nature of their business provides them strong incentives to fend off any competition. If the success of the business is predicated on attracting the largest amount of data possible, to feed algorithms based on the most representative data, it is clear that, for instance, Facebook, Google, or Amazon are the most successful when all potential users are exclusively using their platform. While the tendency toward monopoly has always been an incentive to companies who wish to dominate markets and thus capture higher profits, big data in the very nature of the product makes the creation of monopolies a business imperative—as for instance Silicon Valley veteran Peter Thiel eloquently argues (Thiel & Masters, 2014). It is no surprise that two of the four articles in this special issue deal with this challenge, among other aspects.

Looking at the downstream level, many of the ethical contentions are of course informed by problematic practices in earlier stages of the supply chain. The use and availability of data and the degree of dissemination often interfere and conflict with norms of privacy, transparency, and individual consent. Beyond that, applications and usages of big data, most notably in advertising, can encroach on individuals' personal sphere and psychological privacy. Such encroachment can be even more ethically questionable where big data services change fundamentally the way humans interact, socialize, and take responsibility. The controversy around services such as Snapchat exemplifies those questions. How individuals create and actualize their "digital selves" (Belk, 2013) become increasingly questions of the responsibility of big data businesses—as these processes are almost exclusively controlled by private sector companies.

Finally, looking at the state of the art in how big data companies address these issues, one has to acknowledge that responsible business practices are still very much in its infancy. Of course, initiatives such as the Global Network Initiative (GNI; 2017; mostly as a reaction to the challenges arising from the global operations of these companies) show that the industry has started to address these public concerns—albeit in a rather lukewarm and arms length approach. But ultimately, many of the contentions around the very business model of big data companies and the inherent issues emanating from the novel technologies are hitherto unaddressed. The fact that many of these questions of business responsibility in the industry are currently mostly subject for courts and law enforcement points to the fact that so far little voluntary

corporate initiative has taken place. On top of this, most Internet companies resist or circumvent standardized reporting and accountability measures and largely prefer to develop their own modes of disclosing information, such as the "transparency reports" that Parsons' (2017) article discusses.

These questions about the roles and responsibilities of public and private actors when it comes to developing, operating, and governing digital infrastructures and the resources they command deserve much more scholarly attention. We hope the work published in this special issue will contribute to an increased focus on digital transformations in the field of business and society, and beyond.

Outline of the Special Issue

The first article in this issue, by Sarah Myers West, provides a historical account of the emergence of "data capitalism." Tracing the origins and expansion of commercial uses of data and the worldviews and forms of power they give rise to, the article contributes to emergent scholarship on the role of Internet companies in the reconfiguration of business and society. As West suggests, these developments are made possible through corporate narratives and ideologies that foreground community values, sharing and transparency, and background the forms of information asymmetry, uncompensated labor, and social control at play when data emerges as a key resource for commercial actors.

The article by Glen Whelan contributes to what hopefully will become an emerging stream of literature on big data and social responsibility in a number of significant ways. First, by developing a conceptual framework of categorizing this new phenomenon of big data companies, Whelan provides an opportunity to understand, explain, and critically evaluate these organizations. Combining three hitherto distinct theoretical schools (Foucault, neo-Gramscian, Deleuze & Guattari) the article maps out new conceptual space that might inform and help theorize further work in this area. But it also contributes in wider ways to the business and society literature as it challenges some existing claims in both the Corporate Political Activity (CPA) literature, as well as in the emerging debate on "political CSR." Finally, the article is a great example that the study of this new organizational field asks for a closer dialogue between the business and society literature on the one hand and the Internet governance literature on the other. It thus contributes nicely to one of the initial aspirations motivating this special issue of *Business & Society*.

As in Whelan's article, Jean-Marie Chenou and Roxana Radu (2017) follow a specific case around the monopolist of Internet search, Google.

While this indicates that often in emerging fields research follows the availability of data (hence large organizations provide the best starting point), the article looks more pointedly at the societal governance role of Google. Using longitudinal data, the article highlights how big data companies are changing and powerfully shaping hybrid forms of governance. And while the relatively interventionist approach of the European Commission toward the company in this case is a clear indicator of core ethical issues not yet being addressed, sometimes not even acknowledged, in this new industry, it is also a clear analytical exemplification of the stark power differentials between regulators and private companies due the nature of the underlying technology. The article has a great potential to inform and motivate further studies on how society is now governed not just by the tools, but also the underlying values of these private companies.

This special issue is rounded off by Christopher Parsons' article on emergent forms of reporting in the Internet industry. Taking its point of departure in Canadian telecommunication companies, the article highlights "transparency reports" as an increasingly central mechanism for corporate attempts to show how states carry out surveillance, request information, and otherwise influence the workings of digital spaces. As Parsons suggests, such voluntary forms of disclosure play an important role in the corporate shaping of public perceptions and political discussions of alliances and tensions between governments and the Internet industry, but also suffer from a lack of standardization and possibilities for comparison across companies and settings.

Acknowledgments

All articles in this special issue have been at least double blind reviewed. We would acknowledge the invaluable input and work of all reviewers: Oana Brindusa Albu, Bobby Banerjee, Claire Birchall, Danny Breznitz, Thorsten Busch, Edward Comor, Burkard Eberlein, Peter Edward, Michael Etter, Patrick Haack, Joris von Hoboken, Phil Howard, Dan Kärreman, Arno Koroula, David Lyon, Jukka Mäkinen, Daniel Nyberg, Andreas Georg Scherer, and Christopher Wickert.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

References

Belk, R. W. (2013). Extended self in a digital world. *Journal of Consumer Research*, *40*, 477-500.

Carberry, E. J., Bharati, P., Levy, D. L., & Chaudhury, A. (2017). Social movements as catalysts for corporate social innovation: Environmental activism and the adoption of green information systems. *Business & Society*. Advance online publication. doi:10.1177/0007650317701674

Chenou, J.-M., & Radu, R. (2017). The "right to be forgotten": Negotiating public and private ordering in the European Union. *Business & Society*. Advance online publication. doi:10.1177/0007650317717720

Cohen, B., & Kietzmann, J. (2014). Ride on! Mobility business models for the sharing economy. *Organization & Environment*, *27*, 279-296.

Dashwood, H. S. (2014). Sustainable development and industry self-regulation: Developments in the global mining sector. *Business & Society*, *53*, 551-582.

Deibert, R. (2015). The geopolitics of cyberspace after Snowden. *Current History*, *114*(768), 9-15.

Duhigg, C. (2012, February 16). How companies learn your secrets. *The New York Times*. Retrieved from http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

Duhigg, C., & Barboza, D. (2012, January 25). In China, human costs are built into an iPad. *The New York Times*. Retrieved from http://www.nytimes.com/2012/01/26/business/ieconomy-apples-ipad-and-the-human-costs-for-workers-in-china.html

Etter, M., Colleoni, E., Illia, L., Meggiorin, K., & D'Eugenio, A. (2017). Measuring organizational legitimacy in social media: Assessing citizens' judgments with sentiment analysis. *Business & Society*. Advance online publication. doi:10.1177/0007650316683926

Flyverbom, M. (2016). Disclosing and concealing: Internet governance, information control and the management of visibility. *Internet Policy Review*, *5*(3), 1-15.

Gawer, A., & Cusumano, M. A. (2014). Industry platforms and ecosystem innovation. *Journal of Product Innovation Management*, *31*, 417-433.

Global Network Initiative. (2017). Available from http://www.globalnetworkinitiative.org

Howe, D. C., & Nissenbaum, H. (2009). TrackMeNot: Resisting surveillance in web search. In I. Kerr, C. Lucock & V. Steeves (Eds.), *Lessons from the identity trail: Anonymity, privacy, and identity in a networked society* (pp. 417-436). Oxford, UK: Oxford University Press.

Martin, K. E. (2015). Ethical issues in the big data industry. *MIS Quarterly Executive*, *14*, 67-85.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Boston, MA: Houghton Mifflin Harcourt.

Parsons, C. (2017). The (in)effectiveness of voluntarily produced transparency reports. *Business & Society*. Advance online publication. doi:10.1177/0007650317717957

Richards, N. M., & King, J. H. (2014). Big data ethics. *Wake Forest Law Review*, *49*, 393-432.

Runhaar, H., & Lafferty, H. (2009). Governing corporate social responsibility: An assessment of the contribution of the UN Global Compact to CSR strategies in the telecommunications industry. *Journal of Business Ethics*, *84*, 479-495.

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

Scherer, A. G., Palazzo, G., & Matten, D. (2014). The business firm as a political actor: A new theory of the firm for a globalized world. *Business & Society*, *53*, 143-156.

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

Tan, J., & Tan, A. E. (2012). Business under threat, technology under attack, ethics under fire: The experience of Google in China. *Journal of Business Ethics*, *110*, 469-479.

Tapscott, D. (1997). The digital media and the reinvention of government. *Canadian Public Administration*, *40*, 328-345.

Tapscott, D., & Ticoll, D. (2003). *The naked corporation: How the age of transparency will revolutionize business*. Toronto, Ontario, Canada: Simon and Schuster.

Thiel, P., & Masters, B. (2014). *Zero to one: Notes on startups, or how to build the future*. New York, NY: Crown Publishing.

Treem, J. W., & Leonardi, P. M. (2012). Social media use in organizations: Exploring the affordances of visibility, editability, persistence, and association. *Communication Yearbook*, *36*, 143-189.

Vogel, D. (2010). The private regulation of global corporate conduct: Achievements and limitations. *Business & Society*, *49*, 68-87.

Wareham, J., Fox, P. B., & Cano Giner, J. L. (2014). Technology ecosystem governance. *Organization Science*, *25*, 1195-1215.

West, S. M. (2017). Data capitalism: Redefining the logics of surveillance and privacy. *Business & Society*. Advance online publication. doi:10.1177/0007650317718185

Whelan, G. (2017). Born political: A dispositive analysis of Google and copyright. *Business & Society*. Advance online publication. doi:10.1177/0007650317717701

Zuboff, S. (1988). *In the age of the smart machine: The future of work and power*. New York, NY: Basic Books.

Zuboff, S. (in press). *Master or slave? The fight for the soul of our information civilization*. New York, NY: Public Affairs.

Zwitter, A. (2014). Big data ethics. *Big Data & Society* , *1*(3), 1-6.

Authors Biographies

Mikkel Flyverbom (PhD, Copenhagen Business School) is associate professor at the Department of Management, Society and Communication, at Copenhagen Business School. Recent publications address how the Internet has emerged as a key concern in global politics, how "big data" relates to knowledge production and governance, how transparency ideals shape the Internet domain, and how power and visibilities intersect. His work has been published in leading journals such as *Business & Society, Management Communication Quarterly, Organization, Organization Studies, The*

Information Society, The International Journal of Communication, International Political Sociology, and others. He is currently involved in a major, five-year research project on "Global foresight and anticipatory governance."

Ronald Deibert (OOnt, PhD, University of British Columbia) is professor of political science and director of the Citizen Lab at the Munk School of Global Affairs, University of Toronto. Recent publications include *Black Code: Surveillance, Privacy, and the Dark Side of the Internet* (Random House, 2013), *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace* (MIT, 2010), and articles in *Global Governance, International Organization, Review of International Studies*, and others. He was a cofounder and principal investigator of the OpenNet Initiative and Information Warfare Monitor projects.

Dirk Matten (Dr. rer.pol., Dr. habil., Heinrich-Heine-Universität Düsseldorf) holds the Hewlett-Packard Chair in Corporate Social Responsibility at the Schulich School of Business, York University, Toronto, where he is also associate dean research. He is the director of the Centre of Excellence in Responsible Business. He has published 23 books and edited collections on corporate social responsibility (CSR) and business ethics as well as numerous articles in journals including *Academy of Management Review, Journal of Management Studies*, and *Organization Studies*. He is interested in CSR, business ethics, and comparative international management.