The Crowd and Sensors Era: Opportunities and Challenges for Individuals, Organizations, Society, and Researchers

Completed Research Paper

Sue Newell
University of Sussex
Brighton BN1 9RH, UK
sue.newell@sussex.ac.uk

Marco Marabelli
Bentley University
175 Forest St. Waltham, MA, USA
mmarabelli@bentley.edu

Abstract

In this paper we focus on the consequences of the adoption of new emerging technologies for individuals, organizations, and the wider society. We look at how online collaborations - what we will call the crowd approach - and the availability of digital traces about an individual's activity in large databases - what we will call the sensors approach - can, positively or negatively (yet, disruptively) change many aspects of life. Moreover, we consider how far 'digital traces' can be used by scholars to undertake IT-focused research. We conclude our paper with a research agenda that will hopefully stimulate debate in the IS community related to opportunities and challenges of emerging technologies and how they are used and studied.

Keywords: Knowledge Management Systems; crowd-sourcing; sensors; implicit connectivity; explicit connectivity.

Introduction

Emerging computer technologies (and their applications) are growing exponentially and now pervade the objects we use in both work and private life. These digitized objects are today almost always connected to the internet, and are everywhere – a phenomenon described as ubiquitous computing (Satyanarayanan, 2001). This means that we, and the objects we use in our daily life, are connected to others either explicitly (e.g., when we use Facebook to message our friends or Twitter to send out mass messages) or implicitly (e.g., when our phone tracks where we are) anywhere and everywhere. In this paper we consider this distinction between explicit and implicit connectivity in relation to the implications for individuals, organizations and societies. Explicit connectivity occurs where human actors' explicitly contribute or use content, through some sort of online application (social media, for instance). Implicit connectivity, in contrast, is based on using the data (the digital trace) that is the byproduct of the digitized objects that we use (based on developing algorithms that uncover connections in the data). The difference, then, is in terms of whether we are looking at the actual input of ideas and content from human actors or rather at the data trail from the technology-supported activity. For example, with Twitter people make and read comments on what they are doing or what they think - this is explicit connectivity if it is the content of the tweets that is the focus of use; it is implicit connectivity if the data is used to examine patterns between tweeters and tweets for predicting something else. As another example, just having the smartphone in one's pocket allows data to be collected on where one has visited - this is implicit connectivity where this data is used to predict, for example, what adverts to send to a user, but is explicit connectivity where a user turns on the location function in order to allow friends to know where s/he is. These examples illustrate that it is not the technology or the application that affords implicit or explicit connectivity. Rather, explicit or implicit connectivity depends on whether it is the content (explicit) or digital trace data (implicit) that is used following a person's engagement with different types of technology and applications.

In this paper, then, we look at ubiquitous computing and the associated implicit and explicit connectivity and examine how the content and data is being used and with what consequences (positive and negatives), and thus the challenges and opportunities for individuals, businesses and the wider society. More specifically, in focusing on explicit or implicit connectivity, we contrast two new ways in which organizations are using the content and digital trace data from our era of ubiquitous computing – the crowd and sensor approaches (Newell, 2014). The first 'crowd' approach is based on the emergence of Web 2.0 (or Enterprise 2.0) and the social software applications that have been developed to allow people (including strangers) to connect and share information and knowledge with one another based on some kind of mutual interest or objective (McAfee, 2006). This includes social software applications such as Facebook, LinkedIn, Twitter, but also other types of collaborative platforms such as research forums, wikis, fund-raising websites (crowd-funding) etc. We call this the crowd approach because, especially when applied in an organizational context, the stated purpose of using such platforms is to take advantage of many people's ideas and expertise in order to either identify new opportunities or solve problems; the crowd approach is thus based on explicit connectivity. In many ways, as we will show, the crowd approach is a continuation of the use of IT to share information and knowledge that has been prevalent in the past. It is new in the sense that the scope and range of people involved extends beyond the organizational boundary and to strangers, where previous information and knowledge sharing systems were largely internal to an organization, or included specific partner organizations or individuals. The second 'sensor' approach is based on all the tracking devices that are now embedded in the tools that we use, such as car GPS systems and smartphone apps (including social media apps), that collect digital traces on where someone has visited and who they network with, and wristbands that measure the level of activity. These tracking devices, thus, collect data about our habits, people we see, and places we go and organizations are beginning to use this data to generate knowledge (as when Amazon 'knows' what other books you might be interested in, based on what you have read before and what others who have a similar reading profile have also read). This sensor approach, then, is very different because it uses data analytics (including algorithms and visualization techniques) to generate information and knowledge rather than relying on human actors intentionally sharing their knowledge. We think it is important to consider both the crowd and sensor approaches together because they rely on the same technologies, but use the content and data from these technologies very differently and with different consequences.

We consider the positive consequences of the crowd and sensor approaches to generating information and knowledge but we also identify how both approaches have a 'dark side' that generally is related to unintended consequences. An example for individuals is the irresponsible use of social networks, leading to online bullying or predatory activities (crowd approach), and the discriminations (made by algorithms) that can originate from profiling specific individuals (sensor approach). For organizations, an example of a negative affect of the crowd is manipulated reviews that damage their reputation, and of the sensor approach, ID badges used in the workplace that continuously monitor employees' location and may affect workers' motivation. And at a higher level again, the whole society can be negatively affected by unintended consequences: think about the massive use of social networks leading to 'alienation' and loss of contact with the real world (crowd approach); and the control that institutions (large organizations but also governments) can have over citizens if these institutions are able to monitor the minutiae of peoples' everyday life (sensor approach). Therefore, in this paper we acknowledge the positive aspects of emerging technologies and their uses, but also bring to the fore the urgency of clearly identifying their dark side, aiming to stimulate a constructive debate on how to responsibly exploit the potential of crowds and sensors (and this is our first contribution) while minimizing the 'dark side'.

Along with the identification of opportunities and challenges of the crowd and sensor approaches in business and society, we also reflect on opportunities and challenges for scholars. It has been highlighted that *digital traces* ('records of activity (trace data) undertaken through an online information system', Howison, Wiggins, and Crowston, 2011, p. 769) can be extremely helpful for undertaking, for example, detailed social network research (Kleinburg, 2008) or for studying human-technology interactions and sociomaterial practices (Hedman, Srinivasan, and Lindgren, 2013). Yet, we think that the availability of crowd content and sensor data represents both an opportunity and a challenge for scholars. The opportunity is that this online content and the digital traces can provide very rich and longitudinal datasets, the challenges are a) the difficulty in capturing information about the context and b) the difficulty of capturing emotions. Our aim, in identifying these consequences, is to initiate a discussion on the adoption of online content and digital traces to undertake research, and the extent to which the results are comparable with those undertaken with traditional fieldwork-based data collection (and this is our second contribution). The reminder of the paper articulates the above and provides a rich research agenda that will hopefully stimulate debate in the IS community related to opportunities and challenges of emerging technologies and how they are used and studied.

The Crowd Approach

The crowd approach relates to the use of various types of social software used to enable interactions among many, distributed people (see Yuan et al., 2013). These interactions can either be controlled by the organization – where the organization seeks out inputs from the crowd; or they can be out of the organization's control – where users generate content about an organization and its products and services. So, we can distinguish between organizationally-controlled and user-controlled crowd-sourcing.

Organizationally-controlled Crowd-sourcing

First, in relation to organizationally-controlled crowdsourcing, the assumption is that if an organization does not know the answer to a question, someone out there will; given that we can potentially get answers from many people using social software platforms, we can exploit these to gain access to knowledge that we do not possess; if we ask many and get different answers, we can go with the majority since the 'crowd' will likely have the right answer (Boudreau and Lakhani, 2012). We can thus use the 'wisdom of the crowd' to enable fast and effective open innovation (Chesbrough, and Garman, 2009), for example, using contests to stimulate contributions (Boudreau and Lakhani, 2012). This type of crowdsourcing, in other words, is based on the idea that expertise diversity can generate innovation more effectively than less diversity (Majchrzak and Malhotra, 2013) (with a number of studies across different problem areas demonstrating this advantage, e.g., Boudreau, 2012) and that social software can afford the bringing together of this diverse expertise. In this way, extra- (rather than intra-) organizational knowledge processes come to the fore[1]. For instance, research has focused on how to maximize knowledge sharing in these collaborative social software forums (e.g., Faraj, Jarvenpaa and Majchrzak, 2011), especially in contexts where there may be no immediate gain to those sharing their knowledge and despite potential free-riding of some (e.g., Whelan, 2007; Davison and Ou, 2013). However, as von Krogh (2012) argues, while social software offers considerable promise for managing knowledge, it also 'raises fundamental questions about the very essence and value of firm knowledge, the possibility of knowledge protection, firm boundaries, and the sources of competitive advantage' (p. 154). Rather than knowledge being a precious resource to be shared within the organization to create value, but protected from the outside to achieve competitive advantage, social software and the associated ideas of crowd-sourcing potentially turn this traditional mantra on its head. Utilizing social software for open innovation, thus, needs careful consideration, in particular in relation to how and what knowledge to protect and what to share with others outside the firm. As Smith et al. (2012) note, we should not forget that at times, reducing the barriers to knowledge sharing can have a 'dark side'. Thus, they conducted a study to demonstrate how, in networks of professional practice, confidential company information can be inappropriately disclosed.

While there has been focus on increasing contributions from the crowd, another finding is that most crowd platforms do not encourage co-creation (others commenting on posted ideas). This often leads to a large quantity of posted ideas but then these ideas are not further elaborated collectively (Majchrzak and Malhotra, 2013), thus restricting collaborative discourse which is essential for innovation (Carlile, 2002). Moreover, Bayus (2013) looks at Dell's IdeaStorm (http://www.ideastorm.com) to find that those who

---

[1] Social software can also be used for internal knowledge sharing but here we focus on using the technology to afford access to knowledge outside a firm's boundaries

contribute good ideas through crowd sourcing are those that generate multiple ideas, rather than single ideas. However, both Majchrzak and Malhotra (2013) and Bayus (2013) conclude that once an ideator has had an idea implemented they find it difficult to come up with further valuable ideas for the organization, because their subsequent contributions tend to be very similar to those already implemented.

The above studies, then, suggest that we need to consider how to design social software platforms that best afford crowd participation and the co-creation of actionable knowledge. In this vein, Majchrzak and Malhotra (2013) suggest that co-creation is restricted by three tensions in existing crowdsourcing architectures: 1) simultaneously encouraging competition and collaboration; 2) idea evolution takes time but crowd members spend little time; and 3) creative abrasion requires familiarity with collaborators yet crowds consist of strangers. In response to these tensions, these authors suggest architectures that might better afford the co-creation that is needed for successful crowd-supported knowledge generation. For example, they suggest designing systems that encourage idea evolution rather than simply idea generation and incentivizing contributors rather than just winners of a competition. In this way, IT is not just an enabler of crowd-sourcing but can be designed to shape and optimize open innovation afforded by social software (Majchrzak and Malhotra, 2013) and exploited by organizations; however, as we will illustrate next, crowd-sourcing can be also controlled by users.

User-controlled crowd-sourcing

User-controlled crowd-sourcing refers to the use of social software by the crowd that generates information and knowledge about, rather than for, an organization. Here we are interested in anyone who contributes content and/or comments on something related to an organization. Such crowd-sourcing allows individuals to comment on an organization's products and services, e.g., in the form of reviews or comments on sites like Amazon and TripAdvisor. Such reviews have been found to influence what stakeholders (and in particular customers or potential customers) feel they know about a firm's products or services more than a firm's own market-generated content that attempts to educate customer's only about the benefits of their products and services (Goh, Heng, and Lin, 2013). The literature is still inconsistent about whether crowd reviews on social software platforms can influence purchase behaviors e.g., Mudambi and Schuff (2010) identify a positive effect of online reviews on purchases while Lee, Park, and Han (2011) and Rose, Hair, and Clark (2011) show mixed results. Nevertheless, such online reviews are perceived as a threat by organizations because they can influence their external reputation. Scott and Orlikowski (2013), for instance, note that online reviews lead to reconfiguration of everyday practices of the organization being evaluated. Research suggests that some organizations try to overcome this threat by manipulating reviews (Mayzlin, Dover, and Chevalier, 2013) in order to improve their rating (e.g., on sites like TripAdvisor) (Scott and Orlikowski, 2012). Competitor organizations have also been known to post bad reviews on their rivals in order to achieve some competitive advantage. This has been described as 'sock-puppeting' - creating online identities for the purpose of deception (http://www.nytimes.com/2014/01/09/fashion/Wikipedia-Judith-Newman.html?_r=0). Ethical issues are, thus, prevalent here because the identity of contributors is not always disclosed (Santana and Wood, 2009) even though anonymity might make users more comfortable expressing their opinion freely (Scott and Orlikowski, 2014). Recent research indicates that fake reviews affect a large number of available online reviews. For example, Hu et al (2012) conducted an algorithm-based text analysis on over 600,000 online reviews related to 4,490 books focusing on how writing style changes over time. They found that around 10.3% of the books in their sample are subject to online review manipulation (at least, according to their methodology). This study is interesting because it brings to the fore that 'fake' reviews might be a relatively significant part of all reviews posted on a social network. Yet, as the authors themselves acknowledge, the model they developed to identify manipulated reviews cannot be extended to other products or services, highlighting the urgent need to develop a research agenda addressed to the identification of methods that can be used to detect false reviews across user-controlled crowd sites. Without such research, this type of user-controlled crowd platform will not afford the legitimate user voice that is anticipated. The research agenda, then, needs to focus on ways to afford the positive behaviors that a crowd can make (both that which is organizationally-controlled and that which is user-controlled) while simultaneously reducing its dark side. Jarvenpaa and Majchrzak (2010) have made a start here by identifying the importance of differentiating between 'vigilant' (interactions that cause no harm) and 'non-vigilant' interactions. In doing this, Jarvenpaa and Majchrzak (2010) argue that we need to focus on emergent action-reaction sequences in situations of trust and power asymmetry (where online contributors are not equal and where some, e.g., pedophiles may be interacting deceptively), finding ways to identify contributions that reflect predatory behaviors that may cause harm.

Crowd-sourcing, then, is dynamic (works on web 2.0 platforms) and users' explicit involvement is key for the creation and articulation of content. One consequence of this 'active' involvement of users is that a misuse (or, better, not responsible use) of technology can easily bring up its dark side – this dark side involving various types of problems associated with internet addiction and loss of contact with reality (Leung, 2004), review manipulation, predatory activity and so on. In sum, the crowd approach affects (positively and negatively) individuals, organizations, and society, as we highlight in Table 1.

Table 1. Crowd-sourcing

	Individuals	Organizations	Society
Crowd (positive)	• Posting anonymously makes the poster more 'free' to express ideas (Scott and Orlikowski, 2014)	• Can promote fast and effective innovation since the crowd generally has the right answer (Boudreau and Lakhani, 2012; Chesbrough, and Garman, 2009) • Inter-organizational knowledge sharing that promotes innovation (Faraj, Jarvenpaa and Majchrzak, 2011) • Helpfulness of online reviews for the 'managers' (Scott and Orlikowski, 2012) • (In organizationally-controlled settings) potential for the development (and mostly improvement) of new ideas (Bayus, 2013; Majchrzak and Malhotra, 2013)	• Online reviews generally have positive effects for consumers (Mudambi and Schuff, 2010)
Crowd (negative)	• Technology addiction with individuals spending all their time in the virtual (rather than real) world	• Sharing knowledge (instead of protecting knowledge) might lead to erosion of competitive advantage (Trkman and Desouza, 2012; Smith et al., 2012; von Krogh (2012) • Manipulation of online reviews (Hu et al. 2012) • (In organizationally-controlled settings) online contributions often not subject to development (Bayus, 2013; Majchrzak and Malhotra, 2013)	• Posting anonymously or with fake-IDs opens opportunities for bullying, exploitation (Mayzlin et al., 2013) • Spending too much time in the 'virtual world' can lead to alienation

The Sensors Approach: Big and Little Data

The sensor approach involves using the data trail from social software applications on our mobile devices as well as from other artifacts which increasingly now have tracking and sensing software in them so that 'the digital artifacts will be able to remember where they were, who used them, the outcomes of interactions, etc.' (Yoo, 2010, p. 226). As McAfee and Brynjolfsson (2012) state 'each of us is now a walking data generator' (p. 5). Understanding how sensors and the associated data analytics are being used is extremely relevant to our understanding of the positive and negative consequences of our new era of ubiquitous computing. And just as with the crowd approach, the sensor approach often involves extra- (rather than intra-) organizational interactions. For example, think of the third-party tracking-cookies that are stored in an individual's device and that record and memorize one's visits to websites and suggest similar or associated products and services on other websites, through banners; think of when a cough medication is looked up using Google and, the day after, an 'ad-hoc' ad from CVS (a large US pharmacy) appears, reminding one that it is possible to get a flu-shot anytime without appointment and for only $20. Using sensor data, we argue, can, and arguably already is having, a radically different impact on individuals, organizations, and society and raise some new tradeoffs that we need to consider, as we articulate next.

Sensors and Data Analytics

The data trail from the technologies we use provides the opportunity for data driven decision-making, which McAfee and Brynjolfsson (2012) argue, is superior to traditional 'HiPPO' (highest-paid person's opinion) decision-making, that is from human judgement–based decisions. Data-driven decision-making is based on collecting large quantities of data from the sensors that are now built in to all the tools and technologies that we use in our daily lives and then developing algorithms that can predict particular outcomes (e.g., the numbers of 'friends' on Facebook used to predict a person's credit risk). This data-driven decision-making may derive data from social media used to generate crowd contributions, but it is not based on the content of these contributions, but rather the patterns of connections that can be identified in these contributions. Sensor data can, then, be used to track general trends (big data) as well as the minutiae of an individual's everyday life (little data). Typical devices embedding sensors are smart-phones (with a GPS, for example but also most applications downloaded on the phone collect activity-level data, see Facebook 'check in' feature, for instance); other examples involve car computers that embed a GPS and infotainment systems or toll-both transponders (http://www.usatoday.com/story/money/cars/2013/03/24/car-spying-edr-data-privacy/1991751/). Some of these car sensors are local, meaning that the information is stored in the car's 'black box' and can be extracted by the manufacturer or by licensed car shops. These devices, called EDRs (electronic data recorders), are mostly used for diagnostics associated with engine or electronics problems – yet the information that is saved (and, in some cases, shared remotely) provides details on how drivers operate a vehicle (for instance, average speed, number of times the driver uses the brakes, whether the seat-belts are fastened, etc.). Because of privacy concerns, EDR devices currently overwrite the data after a period, or mileage (e.g., after 1,000 miles), however, infotainment systems and, more generally, onboard computers have the ability to provide real time, two-way connections between the driver and others, for example, the automaker or an insurance company. One example is the OnStar software (www.onstar.com) from GM (General Motors) that provides subscription-based communications, in-vehicle security, hands free calling, GPS, and remote diagnostics in all 50 States in the US and in China. In 2011, OnStar made an announcement that they would start retaining information collected through GPS and onboard systems and that these details could be sold to third parties, most probably insurance companies. GM, then, at the time of writing this paper, seems to be willing to sell anonymized (big) data. However, some have identified privacy issues associated with this. Such privacy concerns are currently at the center of litigation by law enforcement agencies and insurance companies, who want to use such information against drivers, while privacy advocates (including some politicians) are contesting this (http://www.nytimes.com/2014/01/11/business/the-next-privacy-battle-may-be-waged-inside-your-car.html?_r=1).

The above suggests that organizations can analyze big datasets (in combination and often for purposes other than what the original data was collected for – data exhaust) and, based on the connections found, take action even if the causal reasons for the connections are unknown (Mayer-Schonberger and Cukier, 2013). A point to note here is whether we refer to big data and, thus, the use of data to predict general trends, or to little data and, thus, to the use of data to examine a specific individual's behavior through information collected by, for example, a car's GPS, an iPhone, or website activity. While big data analytics is very similar to the more familiar (and less sexy) business intelligence that has been studied for a while, little data (collected through sensors), we argue, deserves particular attention. Figure 1, synthesizes the key differences between big and little data.

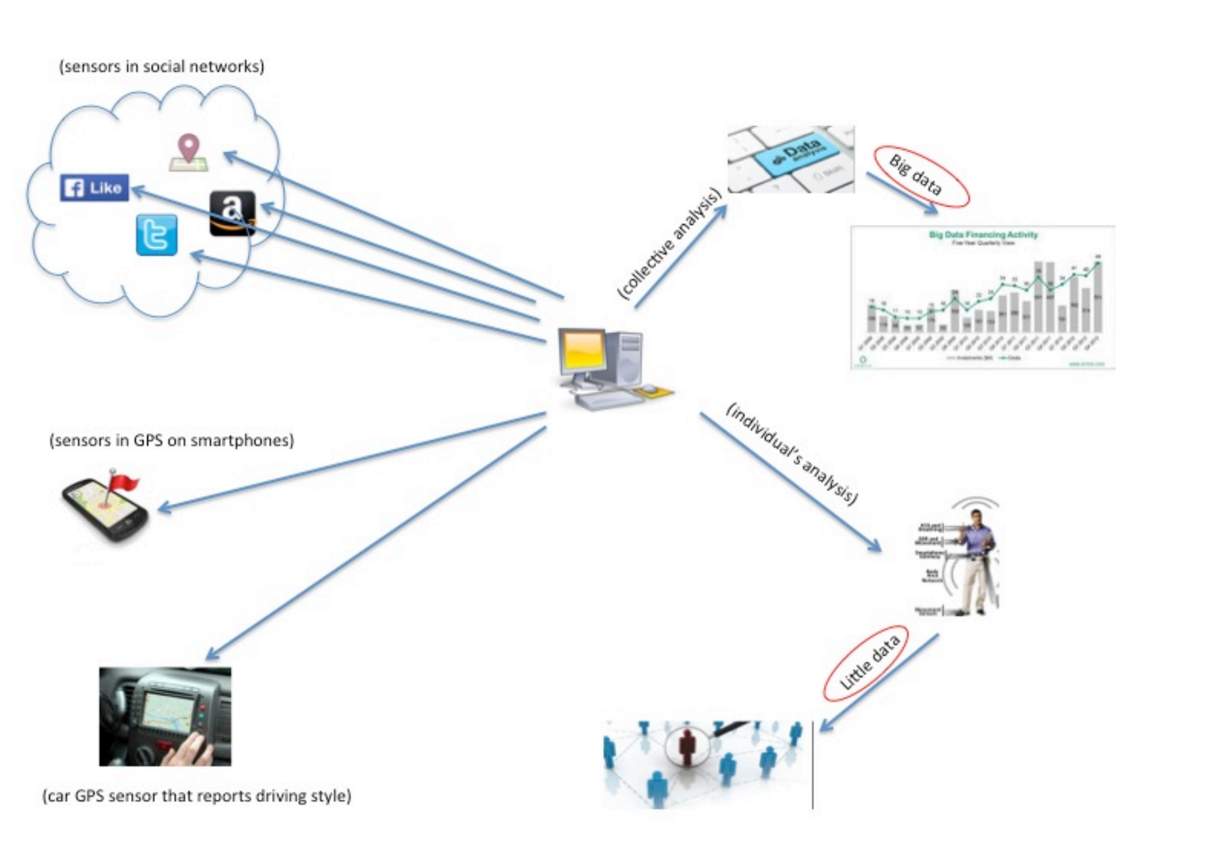

Figure 1. Big and Little Data Collected through Sensors

Little data and Discriminations

Big data involves statistics and analyses aimed at identifying trends, while little data focuses on profiling specific individuals. Think of the previous example of a car's computer that monitors speed, usage of brakes, horn, lights, etc. Looking for general trends based on this sensor data could reveal that most drivers on the Massachusetts Turnpike (a US highway) do not drive faster than 55 miles per hour (the speed limit) in a certain section but data may also show that men on average drive faster than women. Here, we utilize big data to identify a trend and then companies can use this to make discriminations (e.g., charging men higher premiums). Such data-driven trend data has recently been questioned because it appears to go against the value of equal or fair treatment. This is exemplified in the recent case in the EU, where insurers were required to no longer use the statistical evidence about gender differences to set premiums. Thus, despite the fact that gender differences are clear from the data – e.g., young male drivers are 10 times as likely to be killed or injured than those (of both sexes) over the age of 35; women live, on average, longer than men – it is considered to be discriminatory (following an EU ruling that went into effect in December 2012) to use this trend evidence to differentiate between premiums for men and women. The point about this change in the law was that it was considered to be discriminatory because while young men in general, for example, may drive more recklessly and so be more prone to accidents, a specific young man may not and yet is discriminated against when insurers set premiums based on group trends observable in collective data. In contrast to this trend data, sensors can now allow us to concentrate on a specific driver, and we can decide whether s/he is a good or bad driver based on the sensor data from his/her car; in this case we utilize what has been described by some as little data. This can lead to discriminations between individuals (e.g., deciding on insurance premiums) and, importantly, this discrimination (as with the trend data analysis) is made based on computers and algorithms rather than human beings (albeit humans will have determined the algorithm). So, using sensor data, the insurer would not be setting premiums based on the general trends in accident rates between groups, but instead based on the actual driving habits of an individual.

The use of sensor data can have very positive effects on individuals and organizations. For example, they can allow an automaker to identify problems in a car's engine and the problem can be communicated to the car's owner through the onboard computer, perhaps suggesting some dates/times when they can make an appointment with the closest car shop. However, such 'controlling' functionalities can have a 'dark' side, which we discuss next. We suggest that this dark side can be considered in relation to tensions between positive and negative aspects of new sensor-based analysis and decision-making that manifests as tradeoffs, two of them being privacy vs. security and control vs. freedom.

Privacy vs. Security

Sensors can contribute to security: one example is security tracking systems adopted for prison populations, with prisoners released but wearing a tracking ankle-bracelet, which probably improves the overall security of our society, with the sensor acting as a deterrent for prisoners to escape or commit a crime when they are out on parole. Other (potential) positive effects of sensors where security aspects prevail over privacy concerns are the capacity of sensors to trace a stolen phone, or being able to apportion blame in a traffic accident because it is all 'caught on tape', for example with Goggle Glass. In terms of locating a lost phone it has to be the user who, deliberately, accepts 'giving up' her/his privacy by activating the 'find my phone' option. The example of Google Glass is more complex since the privacy that a user gives up affects others' privacy, thus representing a shift from the individual to the societal level, and this is probably what should be a major concern for the use of sensor data. That is, in some circumstances one's use of sensors affects others' privacy, as for example, for people who are 'tagged' in somebody's Facebook profile without them knowing. Some organizations are trying to implement 'work-arounds' to this particular dark side of sensors: Facebook no longer allows a user's 'wild tagging' and, instead, an automatic email is sent to a user who is tagged, for approval. Yet, the exponential diffusion of sensors, embedded in social networks such as Facebook and many other objects leads us to think that it will be hard for organizations (or institutions) to regulate how individuals can use sensors responsibly; in other words, it is unrealistic to think that sensor-equipped devices will always have options to protect others' privacy, for the simple reason that most sensors are not centrally managed and whether or not an individual is exposed to privacy violations lies in the way others use the sensor-equipped tools (think of Google Glass). Thus, the negative aspects of sensors might encourage us to give up some security as the price we want to pay for maintaining more privacy. For example, tracking our children's every movement might allow us to feel that they are safer. However, the loss of their privacy might have far-reaching effects, for instance in terms of their feelings of personal responsibility. After all, we know that punishment is not always an effective deterrent because once the punishment is removed the individual often resorts to the prior (undesirable) behavior; so if individuals conform only because they know they are being monitored, will their behavior change once the monitoring is stopped? That is, with monitoring, like punishment, we are changing the behavior but not the beliefs about what is appropriate or inappropriate behavior (Podsakoff, Todor and Skov, 1982). Thus, whether sensors are used in a positive or negative way is not just an 'institutional responsibility', because large organizations that make available sensor-based technologies cannot fully discipline how we use these sensors. Instead, it looks like we (individuals, as members of our society) have to contribute to responsible sensor-use to find a 'socially acceptable' balance between privacy and security, and this might require a social network or sensor-activated object use 'etiquette', in addition to new laws and regulations. Research examining this trade-off between security and privacy and the implications for individuals, organizations and societies will be extremely important moving forward.

Control vs. Freedom

The datification of everything means that we can use devices to constantly track every decision and place that a person visits (be they an employee, our child or our ageing parent), and use this data to monitor and control (or some now prefer to use the term 'nudge') behavior (Whitman, 2011). Little data can be used by companies to discriminate in what they offer to different individuals through advertising or it can be used by employers to monitor (or, better, control) individual worker performance and then discriminate in terms of rewards. Behaviors can be controlled through constant monitoring of the smallest details of our everyday life, with penalties given for not conforming, by either employing organizations or governments. While this might improve short-term productivity or civil behavior, it might do so at the expense of individuals feeling that they have some freedom and autonomy, feelings which we know have a significant influence on motivation in the long-term (Hasan and Subhani, 2011). One example is Hitachi's new digital identification badge that collects data on employee's exact location within an office, records who the person has spoken to, for how long and how energetically (http://www.cnn.com/2014/02/02/opinion/greene-corporate-surveillance/). This constant monitoring may, however, affect employees' capacity to produce disruptive innovation. In fact, breakthrough innovation is more risky and might lead to more frequent 'failures' (O'Reilly and Tushman, 2004), and individuals constantly monitored are less likely to expose themselves to failures in front of peers and superiors. This suggests that responsible analytics might encourage not tracking employees', customers' or citizens' every movement, this being the price we might want to pay for allowing people to feel in control of the decisions they make – informated and not automated using the language of Zuboff (1984).

While from the above we have learned that in certain contexts, adopting new technologies to control individuals might have negative consequences, a responsible use of sensors, for instance, can also lead to positive consequences for individuals as well as the society. One example is Hsu and colleagues (2012), who conducted an experiment involving reading concentration monitoring systems embedded in e-books. The aim of the research was to demonstrate that these systems, if used in schools, could help instructors measure the reading concentration rate of students in order to address issues related to learning disabilities. Another example that suggests that using sensors responsibly can lead to positive consequences comes from healthcare: eNeighbor (among others) is a wireless service with devices able to monitor a person's motions 24/7 and was proven to be an excellent support to keep the elderly safe. A device is installed under the bed of the person and is activated once s/he wakes up in the morning. Motion detectors in the bedroom and bathroom register that the person has not left the area in her/his usual pattern and send this information to the central monitoring system, prompting a call to the person's house phone to ask if everything is fine. If the person does not pick up the phone, at first a neighbor is alerted, and in case the person does not answer the door, a 911 call is made that dispatches firefighters (http://www.nytimes.com/2009/02/13/us/13senior.html?pagewanted=all&_r=0). Interestingly, while these monitoring systems seem to be effective in the case of individual emergencies (little data), the application of big data technologies on RPM (Remote Patient Monitoring) to identify root causes of diseases and, more generally, to produce advances in clinical research, have produced, so far, mixed results (Chaudry et al. 2010). Nevertheless, it is clear that using sensor data can produce positive consequences. But, as we have seen, in creating these positive consequences there may well be a tradeoff between control versus freedom and research that examines the consequences of managing this tradeoff in different ways may help with the responsible exploitation of sensors.

Finally, another dark side of the sensor era is associated with technology breakdowns. We increasingly rely on sensors for many activities, for example, parking our car and soon even driving our car. However, this might also lead to a change in our ability to manage such activities without sensors. Thus, once our car parks itself, will we forget how to park on our own? In other words, with sensors increasingly influencing and even managing our lives this may occur at the expense of our ability to improvise and respond to emergencies. Thus, as car drivers who now rely on sensors, we do not have the luxury that airline pilots do, of practicing in simulators to ensure that we maintain our skills so that we are prepared for an emergency. This raises another relevant social issue (and tradeoff – between safety and learning) that lets us think about a dark side of ubiquitous computing in peoples' everyday lives (Satyanarayanan, 2001). It also raises the issue of the role of business in promoting such technologies – does business have a responsibility for thinking about such consequences and building in opportunities for learning?

Given the above, we can argue that the datification capacity behind the embedding of sensors will increasingly affect all our lives, both positively and negatively. While Table 2 provides examples of risks and benefits of sensors, in the next section we focus on the relevance of human agency in data analytics.

Table 2. A Multi-level Perspective of Sensor-based Technologies

	Individuals	Organizations	Society
Sensors (positive)	• Control over minors by parents creates a feeling of 'safeness' • Monitoring a student's learning progress (Hsu et al., 2012) • Relying on sensors is positive in that it can saves time (iPhone maps and easiness to reach a particular destination)	• Improving control over the employees' work tasks that leads to efficiency (Podsakoff, Todor and Skov, 1982) • Decision making processes are quicker because they are data driven (Mayer-Schonberger and Cukier, 2013) • Data driven forecast can account for a wide number of variables and allows detailed customer profiling/segmentation (Mayer-Schonberger and Cukier, 2013)	• Sensors to keep people safe • Extreme reliance to sensors
Sensors (negative)	• Monitoring children could lead to a feeling of loss of personal responsibility • Relying too much on sensors (e.g., GPS embedded in the smart-phone) and when a technology breakdown occurs, people are less capable to make autonomous decisions • Personal data from sensors are used for customer segmentation without explicit consent (e.g., iPhone locators and *likes* on Facebook) (Whitman, 2011) • Data driven decision making can lead to individuals' discrimination (see example of car insurance companies in the EU)	• Improving control over the employees' work tasks does not necessarily changes their believes (what they would really do if they were not controlled) (Podsakoff, Todor and Skov, 1982) • Implementing controls that reduce the employees' capacity to produce breakthrough innovation because the employees do not want to take the risk of exposing themselves to failure • Improving control over the employees' work tasks might negatively affect job motivation and satisfaction (Hasan and Subhani, 2011) • Data driven decision making does not provide a reason why a decision is made; this is against processes of organizational learning • Data analyst who does not know anything about the data themselves	• Private citizens needs to have their privacy protected against social discrimination • Unexpected technology breakdowns that involve public services (airports, public transportation) • Hidden control over collectives (e.g., by institutions)

The Role of Algorithms and Implications for Knowledge and Work

Thinking about developments in data analytics based on digital trace data from sensors, we can see that the algorithms that have been created are focused on making discriminations to improve decision-making, the essence of knowledge work (Davenport, 2005). The use of algorithms to make discriminations has the potential to transform work in all kinds of organizations and contexts, including professional or knowledge work. The previously discussed crowd approach uses new technologies to provide actors with a discursive platform through which to share ideas and knowledge that may be relevant to a focal organization. This may reduce the numbers of employees needed – if the crowd can provide input previously the province of employees. However, the sensor approach is more disruptive because discriminations are based on algorithms rather than explicit human content. Those providing the data do not (generally) provide it intentionally and have no say in how their data is used to generate the algorithms that will be the basis of the decision-making. Humans must decide what to measure and produce the algorithms to analyze the data that is collected. However, this does not necessarily involve understanding the causes and consequences of particular patterns of behavior that are identified, rather it is sufficient that connections are discovered. So, traditionally, making discriminations has been a human-centered activity (even if supported by an 'equipped context', Gherardi, 2012), but under the sensor approach these discriminations are based on programed algorithms and the knowledge worker is the data analyst. Moreover, while in traditional knowledge work, that continues to be manifest in the crowd approach, the human actors involved articulate the rationale for their decision (exposing the knowledge basis of their judgment), but in the sensor approach the underpinning rationale is not articulated (and may not even be known) so that the legitimacy of the knowledge on which decisions are made is not easily subject to contestation, nor to development. Indeed, one could argue that the last financial crisis was a product of this problem, with the algorithms that predicted the pricing for mortgage-backed securities clearly not taking into account all the risks but not subject to question because the basis of the algorithm was not accessible.

McAfee and Brynjolfsson (2012) contend that experts in a particular field are still needed because it is these experts who will identify the interesting and useful questions to ask (they cite Pablo Picasso's famous saying 'computers are useless, they can only give you answers'). Thus, knowledge in a particular field is crucial for defining the problems and questions that underpin using data to inform decision-making since 'blind' data analytics can lead to the identification of connections that are not meaningful or that over-simplify and so create unfair or unjust discriminations. The financial crisis, however, illustrates that 'blind' analytics may be all too common. Moreover, McAfee and Brynjolfsson (2012) also predict the growing importance of the big data analyst, an individual who has more than simply statistical knowledge but can also clean and organize the unstructured data (big data is not the sort of data that resides in a carefully constructed database), can develop and use visualization tools and techniques (Leonardi, 2012), can design experiments that can help to tease out causations from correlations, and can speak the language of business so that they can help business leaders formulate the challenges they face in ways which big and little data can help.

This view that using data from sensor technologies for decision-making requires both domain-based business knowledge and data analytics knowledge contradicts the view of some of the 'pure' big data advocates like Mayer-Schonberger and Cukier (2013) who argue that, sometimes at least, using non-experts can be helpful so that they do not read into the data what they want to see, based on their prior knowledge, that can represent a lock-in or path dependency affecting objective evaluations (Cohen and Levinthal, 1990). But even if we accept that both types of knowledge are needed to use sensor -based data, we should not under-estimate the difficulties that this might imply, given the epistemic differences (Knorr-Cetina, 1999) between traditional knowledge workers using a more theoretical/experience-based approach to problem-solving and decision-making and the data analysts algorithmic approach. Moreover, it would seem likely that far fewer domain experts would be needed than currently, since once the algorithm is created based on their knowledge, decisions can be made without them.

Of course, we can overstate the ubiquity of sensor- led automated decision-making; it is unlikely that medics will be replaced in the diagnostic process completely by a pre-programed algorithm that uses data from a sensor on the human subject (see, e.g., Sony's idea about a SmartWig that will be packed with sensors measuring bodily functions). However, the ever-increasing trend of measuring the minutiae of our lives will have consequences for work, including knowledge work, and it is vital that we study this, taking a multi-disciplinary approach that considers, for example, economic, legal, ethical, organizational, societal, and psychological consequences for different populations. In doing this, we should remember that implicit connectivity is not neutral in terms of its consequences for the human actors who leave digital traces that are then collected and analyzed; there are choices about how and what digital traces, (sensor data) are collected and measured, and choices about the algorithms that are developed to make decisions based on this measurement; and these choices raise fundamental social questions. As researchers we have an opportunity to expose this empirically and theoretically and so promote an agenda of 'responsible analytics' that attempts to reduce the negative consequences of this new sensor era.

With the above we have highlighted how new technologies can subvert the traditional approaches to managing knowledge and making decisions, even if they incorporate positive as well as negative implications for individuals, businesses and the wider society. One last point, that we articulate next, is related to how the utilization of data originating from crowds and sensors might affect future research.

Crowd and Sensors Approaches: Opportunities and Challenges for Researchers

Opportunities for Researchers

It is clear that data collected through crowds and sensors can be extremely rich in that they document the minutiae of an individual's everyday life. IS scholars have recognized the opportunity of using online data for research purposes. For instance, Kleinburg (2008), who focused on big data analytics, noted that social networks such as Facebook and LinkedIn offer glimpses of everyday life with a level of granularity that is not even comparable with what 'traditional' data collection on social networks could do; this is particularly interesting if we think that collecting social network data is very time consuming, requires extensive contact with the group of people being studied, and that the data make sense only if almost 100% of the sample (included in the social network boundaries) participates in the study (Wasserman, 1994). Therefore, big data analytics applied to social networks should be seen, Kleinburg argues, as a very positive science advance, since 'we can take something that was once invisible and make it visible' (p. 66). Using datasets on users' behaviors along with an algorithm language for modern social processes, Kleinburg continues, will help make progress on key social science questions, informed by a computational perspective. Howison, Wiggins, and Crowston (2011), in line with Kleinburg, acknowledge the value of *digital traces*, and highlight that social network data collected using digital traces can be more complete than traditional social network data collection, since the latter technique captures (with e.g., a survey) only those links that participants in the study want to highlight (answering specific questions) while the former records every interaction between participants that use a specific social network. Yet, Howison and colleagues recognize a number of critical validity issues associated with using digital traces. In particular, they highlight that it can be problematic to compare social network analyses conducted with traditional methods (survey) with those conducted using digital traces, even though 'digital traceability' (Venturini and Latour, 2010) provides opportunities to study an individual's (or a social network's) everyday life evidence (but excluding the non-captured activities).

Hedman, Srinivasan, and Lindgren (2013) also indicate some of the opportunities from having access to digital trace data, suggesting that this can be extremely helpful for capturing a variety of interactions among humans and between humans and technologies, highlighting that, for instance, studies on sociomaterial practices can benefit from digital traces. Although Hedman and colleagues start from premises that are different than Kleinburg et al. (2011), they come to similar conclusions, pointing to the difficulty of comparing sociomaterial practices captured with observations and interviews with the same practices captured through online social networks or sensors. Here we would like to take this issue further and reflect on whether (and, to what extent) crowd content and sensor data will be able to shed light on research on human-technology interactions that develop over time (following process-oriented frameworks, see Oborn, Barret, and Davidson, 2011), such as sociomaterial practices, discussed next.

Main Challenges

Firstly, we agree that data collected through explicit and implicit connectivity might uncover opportunities for studying human-IT interactions. In fact, this type of research traditionally requires longitudinal and detailed fieldwork, examples being studies that look at how sociomaterial practices (interwoven interactions between human and material agency) evolve and are re-produced over time (Feldman and Orlikowski, 2011; Orlikowski and Scott, 2008). For instance, Suchman developed an ethnographic study involving her experience at Xerox's Palo Alto Research Center where she was employed for 22 years and she covered the position of Principal Scientist and Manager of the Work Practice and Technology laboratory. In her book 'Plans and Situated Actions: The Problem of Human-machine Communication' (1987 and 2007) Suchman presents meaningful details about human-computer interactions that could only be captured through a systematic and longitudinal engagement in fieldwork. However, given that empirical studies on sociomaterial practices are known for being very time consuming (Orlikowski, 2010; Wagner, Moll, and Newell, 2012), data from the technologies we now use provide incredible opportunities for researchers who aim to collect and analyze everyday life details on interactions between people (human agency) and technologies (material agency). However, here we bring to the fore two mayor concerns that in our opinion, represent challenges for scholars. The first is about the lack of contextual variables associated with digital traces (why and how individuals interact with IT in a specific way) and the second is about the incapacity of digital traces to capture human emotions. Both points are elaborated next.

The 'context' issue

As we have illustrated above, traces from individual's behavior (implicit sensor data) and their ideas (explicit crowd contributions) can be captured over time, with a good degree of accuracy, and a high level of data granularity. This is especially so in terms of sensors. For example, an EDR installed on a car can capture, in detail, the 'habits' of a driver. However, what this data may not show is the context that influences this driving habit. Thus, we do not know if a driver obeys the laws because s/he thinks that it is good and safer to respect speed limits or because speed limits are enforced (or because of other contextual variables). It is possible to implement sensors that monitor the whereabouts of a driver and, thus, whether or not controls such as speed cameras are installed, whether the driver carries a passenger (this can be a source of distraction, as well as a way to discipline the driver), whether the driver is 'in rush' (for instance, we can collect information about the driver's job and can easily figure out these details looking at the time and the route), and so on. However, we must ask whether this is realistically possible? Would our society and institutions accept such an in-depth monitoring of people's lives? There are indications that such massive privacy invasion is not welcome. For example, InBloom was a start-up company that planned to collect and integrate student attendance, assessment, disciplinary, and other records from various school-district databases with the aim of putting the data in a cloud and releasing it to authorized web services and apps that could help teachers track each student's progress (https://www.inbloom.org). The program faced strident opposition from a number of parents and privacy advocates and ended up being shut down (http://www.nytimes.com/2014/04/27/technology/a-student-data-collector-drops-out.html).
Institutions too, seem to have started to take a stance towards protecting (or, at least regulating) citizens' privacy against the proliferation of 'wild' data collection and analyses from the digital data traces that we leave. For instance, on May 1st 2014 the White House released a report that recommends developing government limits on how private companies (such as Google and Facebook) make use of the torrent of information they gather from their online customers. Interestingly, one of the six policy recommendations explicitly raises a red flag on potential discriminations: data from sensors can be easily used in subtle ways to create discriminations and, more importantly, to make (sometimes wrong) judgments, about who is likely to show up at work, pay a mortgage on time, or require expensive healthcare treatment. Therefore, this technology has 'the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education, and the marketplace' (http://www.nytimes.com/2014/05/02/us/white-house-report-calls-for-transparency-in-online-data-collection.html?_r=0). And in Europe, Google has been instructed that it must remove from searches information that an individual requests to be removed. All this should lead us to reflect about the feasibility of using data from sensors that monitor, with great detail, the minutiae of individual lives. Thus, studies that aim to analyze sociomaterial practices using digital traces will need to deal with issues associated with the partial view of contextual variables that these 'traces' provide. Thus, we believe that the 'context' issue should be a key subject of discussion among scholars. The 'emotion' issue is another challenge for scholars who utilize digital traces.

The 'emotions' issue

Human-IT interactions that develop in practice over time are best captured longitudinally (Leonardi, 2012), since by definition practices are undertaken on a daily basis, and are continuously re-produced and re-configured (Gherardi, 2009); Leonardi (2011), for instance, suggests that sociomaterial practices are imbrications that evolve constantly (Ciborra, 2004), where the social and material are complementary – like the tegula and the imbrex (rephrased from Leonardi, 2011, p. 150). Moreover, recent research has highlighted that thoughts and emotions play a role in these emerging patterns of interaction (Ortiz de Guinea and Markus, 2009; Stein et al. 2012). This is interesting because if we think of utilizing digital traces (from crowd-sourcing, as well as from sensors) to shed light on sociomaterial practices, it is, at best, challenging to try and capture emotions, feelings, and any kind of sentiment experienced by individuals in their daily enactment of (sociomaterial) practices. However, divorcing the study of IT use from its socio-emotional context would leave us with a very partial view of human-technology interactions (Stein et al. 2012), especially if we aim to look at the evolution of such interactions around continued use of IT (Stein, Galliers, and Markus, 2013), thus, longitudinally. Therefore, here we would like to bring to the fore this second issue associated with utilizing digital traces to study human-IT interactions and practices, and we believe that scholars should take these issues seriously, and reflect on the extent to which it is possible to draw from crowd and sensor approaches to carry out research on such topics. Table 3 summarizes the opportunities and challenges of our era of ubiquitous computing for scholars.

Table 3. Research Adopting Digital Traces: Opportunities and Challenges for Scholars

Opportunities	Challenges
• Availability of large amount of data, already in digital format, and easily analyzable • Data can be captured longitudinally • Results from 'traditional' fieldwork on, e.g., the adoption of new technologies can be compared, to test the validity of the latter • Granularity of details on individuals' behaviors	• Crowd/sensors capture only a limited number of contextual variables • It is unrealistic to think that sensors can be implemented that are able to capture all contextual variables (for privacy issues, it would be simply socially unacceptable) • Crowd-sourcing and sensors (unlike observations) do not capture emotions and thoughts that are key to answer how/why questions

Research Agenda and Concluding Remarks

In this paper, we have attempted to bring to the fore some issues associated with the development of new technologies, which, in our opinion, deserve attention. In particular, we focused on how online collaborations (i.e., the crowd approach) and the availability of digital traces about an individual's activity in large databases (i.e., the sensors approach) can disruptively change many aspects of life, both within organizations and more generally across societies. Despite a few studies that concentrate on some problems related to crowd-sourcing (e.g., Hu, Liu, and Sambamurthy, 2011; Jarvenpaa and Majchrzak 2010), the IS community has been relatively silent in terms of analyzing the emerging issues associated with the adoption of sensors, and the resulting decision-making based on algorithms rather than human knowledge and expertise. Thus, we have argued that implicit connectivity raises a number of social concerns associated with how discriminations are being made, this time by computers instead of people – and these types of discriminations affect business and society as well as individuals. We have also identified methodological issues that, if not properly addressed can compromise research conducted using digital traces.

We believe that the above issues – involving individuals, organizations, society, and researchers – are extremely relevant research topics for us as an IS community, whether we are interested in finding ways to increase business value or we are concerned with broader social issues of equality and democracy (and, of course, business and social values cannot be achieved independently of each other). The issues, affordances, and challenges discussed here pose real dilemmas for organizations (and societies) attempting to exploit the wisdom of the crowd and the datafication of everything. Thinking about these big issues in the era of ubiquitous computing requires that we engage with broader debates about the consequences of technology in business and society. Moreover, while this new era provides opportunities for researchers, we also need to discuss how we can effectively utilize the online content and digital trace data to further explore human behavior and the interactions between people and technology. In conclusion, developing a research agenda around these key points is, we believe, imperative.

References

Alavi M., Leidner D. (1999). Knowledge Management Systems: Issues, Challenges, and Benefits, Communication of the Association for Information Systems, 1, pp. 2-36.

Bayus B. L. 2013. Crowdsourcing New Product Ideas Over Time: An Analysis of the Dell IdeaStorm Community, Management Science, 59(1), pp. 226-244.
Boudreau K. J., Lakhani K. R. (2012). How to Manage Outside Innovation, Magazine: Summer 2009, available online at http://sloanreview.mit.edu/article/how-to-manage-outside-innovation/, last time accessed on Oct 12 2013.
Boudreau, K.J. (2012). Let a thousand flowers bloom? An early look at large numbers of software app developers and patterns of innovation. Organization Science, 25, 5, 1409-1427.
Carlile P. (2002). A Pragmatic View of Knowledge and Boundaries: Boundary Objects in New Product Development, Organization Science, 13(4), pp. 442-455.
Chaudhry S. I. et al. (2010). Telemonitoring in Patients with Hearth Failure, New England Journal of Medicine, 363, pp. 2301-2309.
Chesbrough H. W., Garman A. R. (2009). How Open Innovation Can Help you Cope in Lean Times, Harvard Business Review, 87(12), pp. 128-140.
Cohen W. M., Levinthal D. A. (1990). Absorptive Capacity: A New Perspective of Learning and Innovation, Administrative Science Quarterly, 35(1), pp. 128-152.
Cook S. D., Brown J. S. (1999). Bridging Epistemologies: The Generative Dance Between Organizational Knowledge and Organizational Knowing, Organization Science, 10(4), pp. 381-400.
Davenport T. H. 2005. Thinking for a Living: How to Get Better Performance and Results for Knowledge Workers, Harvard Business School Press, Boston, MA.
Durcikova A., Fadel K. J., Butler B. S., Galletta D. F. (2011). Research Note – Knowledge Exploration and Exploitation: The Impacts of Psychological Climate and Knowledge Management Systems Access, Information Systems Research, 22(4), pp. 855-866.
Davison R. M., Ou C. X. J. (2013). Information Technology to Support Informal Knowledge Sharing, Information Systems Journal, 23(1), pp. 89-109.
Faraj S., Jarvenpaa S. L., Majchrzak A. (2011). Knowledge Collaboration in Online Communities, Organization Science, 22(5), pp. 1224-1239.
Gheradi, S. 2012. How to Conduct a Practice-Based Study: Problems and Methods. Cheltenham, UK: Edward Elgar.
Goh K., Heng C., Lin Z. 2013. Social Media Brand Community and Consumer Behavior: Quantifying the Relative Impact of User- and Marketer-Generated Content, Information Systems Research, 24(1), pp. 88-107.
Orlikowski W. J. (2007). Sociomaterial Practices: Exploring Technology at Work, Organization Studies, 28(9), pp. 1435-1448.
Orlikowski W. J. (2010). Practice in Research: Phenomenon, Perspective, and Philosophy, in Golsorkhi D., Rouleau L., Seidi D., Vaara E. 2010. Cambridge Handbook of Strategy as Practice, Cambridge University Press, Cambridge, MA, USA.
Grant R. M. (1996). Towards a Knowledge-based Theory of the Firm, Strategic Management Journal, 17, pp. 109-122.
Hansen M. T., Nohria N., Tierney T (1999). What's Your Strategy for Managing Knowledge? Harvard Business Review, March-April, 1-11.
Hasan, S. and Subhani, M. (2011). Top Management's Snooping: Is sneaking over employees' productivity and job commitment a wise approach. African Journal of Business Management, 6, 14, 5034-5043.
Hedman, J., Srinivasan, N. and Lindgren, R. (2013). Digital traces or information systems: Sociomateriality made researchable. ICIS, Milan.
Hislop D. (2013). Knowledge Management in Organizations, Oxford University Press, UK.
Howison, J., Wiggins, A., and Crowston, K. (2011). Validity Issues in the Use of Social Network Analysis with Digital Trace Data, Journal of the Association of Information Systems, 12(12) art. 2.
Hu N., Liu L., Sambamurthy V. 2011. Fraud Detection in Online Consumer Reviews, Decision Support Systems, 50(3), pp. 614-626.
Hu N., Bose I., Koh N. S., Liu L. (2012). Manipulation of Online Reviews: An Analysis of Ratings, Readability, and Sentiments, Decision Support Systems, 52, pp. 674-684.
Hsu C., Chen H., Su Y., Huang K., Huang Y. (2012). Developing a Reading Concentration Monitoring System by Applying an Artificial Bee Colony Algorithm to E-books in an Intelligent Classroom, Sensors, 12, pp. 14158-14178.
Jarvenpaa S. L., Majchrzak A. (2010). Research Commentary – Vigilant Interaction in Knowledge Collaboration: Challenges of Online User Participation Under Ambivalence, Information Systems Research, 21(4), pp. 773-784.

Knorr-Cetina, K. (1999). Epistemic Cultures: How the sciences make knowledge. Harvard University Press.
Kogut B., Zander U. (1996). What Firms Do? Coordination, Identity, and Learning, Organization Science, 7(5), pp. 502-218.
Lee J., Park D., Han I. 2011. The Different Effects of Online Consumer Reviews on Consumers' Purchase Intentions Depending on Trust in Online Shopping Malls: An Advertising Perspective, Emerging Marketing Case Studies, 21(2), pp. 187-206.
Leung L. (2004). Net-Generation Attributes and Seductive Properties of the Internet as Predictors of Online Activities and Internet Addiction, CyberPsychology & Behavior, 7(3), pp. 333-348.
Leonard P. M. (2012). Car Crashes without Cars: Lessons about Simulation Technology and Organizational Change from Automotive Design, The MIT Press, Cambridge, MA.
Majchrzak A., Malhotra A. (2013). Towards and Information Systems Perspective and Research Agenda on Crowdsourcing for Innovation, Journal of Strategic Information Systems, 22(4), pp. 257-268.
March J. G. (1991). Exploration and Exploitation in Organizational Learning, Organization Science, 2(1), pp. 71-87.
Mayer-Schonberger V., Cukier K. (2013). Big Data: A Revolution that Will Transform how We Live, Work, and Think, Houghton Mifflin Harcourt Publishing Company, New York, NY.
Mayzlin D., Dover Y., Chevalier J. A. 2013. Promotional Reviews: An Empirical Investigation of Online Review Manipulation, Working Paper N. 18340 available at http://www.nber.org/papers/w18340, last time accessed on January 9th 2013.
McAfee, A. (2006). Enterprise 2.0: The dawn of emergent collaboration. Sloan Management Review, 47, 3, 20-28.
McAfee, A., Brynjolfsson, E (2012). Big Data: The management revolution. Harvard Business Review, October.
Mudambi S. M., Schuff D. 2010. What Makes a Helpful Online Review? MIS Quarterly, 34(1), pp. 185-200.
Nahapiet J., Ghoshal S. 1998. Social Capital, Intellectual Capital, and the Organizational Advantage, Academy of Management Review, 23(2), pp. 242-266.
Oborn, E., Barrett, M., and Davidson, E. (2011). Unity in Diversity: Electronic Patient Record Use in Multidisciplinary Practice, Information Systems Research, 22(3), pp. 547-564.
O'Reilly C. A., Tushman M. L. (2004). The Ambidextrous Organizations, Harvard Business Review, April 2004, pp. 1-10.
Ortiz de Guinea A., Markus M. L. (2009). Why Break the Habit of a Lifetime? Rethinking the Role of Intention, Habit, and Emotion in Continuing Information Technology Use, MIS Quarterly, 33(3), pp. 433-444.
Podsakoff, P., Todor, W., Skov, R. (1982). Effects of leader contingent and noncontingent reward and punishment behaviors on subordinate performance and satisfaction. Academy of Management Journal, 1, 25: 4, 810-821.
Polanyi M. (1958). Personal Knowledge: Towards a Post-critical Philosophy, Routledge & Kegan Paul Ltd.
Pollet T. V., Roberts S. G. B., Dunban R. I. M. 2011. Use of Social Network Sites and Instant Messaging Does not Lead to Increased Offline Social Network Size, or Emotionally Closer Relationships with Offline Network Members, Cyberpsychology, Behavior, and Social Networking, 14(4), pp. 253-258.
Rose S., Hair N., Clark M. 2011. Online Customer Experience: A Review of the Business-to-Consumer Online Purchase Context, International Journal of Management Reviews, 13(1), pp. 24-39.
Santana A., Wood D. 2009. Transparency and Social Responsibility issues for Wikipedia, Ethics of Information Technology, 11, pp. 133-144.
Satyanarayanan, M. (2001). Pervasive computing: vision and challenges. Personal Communications, IEEE, 8, 4.
Scott S. V., Orlikowski W. J. (2012). Reconfiguring Relations of Accountability: Materialization of Social Media in the Travel Sector, Accounting, Organizations, and Society, 37(1), pp. 26-40.
Scott S. V., Orlikowski W. J. (2013). What Happens When Evaluation Goes Online? Exploring Apparatuses of Valuation in the Travel Sector, Organization Science, articles in advance.
Scott S. V., Orlikowski W. J. (2014). Entanglements in Practice: Performing Anonymity Through Social Media, MIS Quarterly, Forthcoming.
Smith A. L., Baxter R. J., Boss S. R., Hunton J. E. (2012). The Dark Side of Online Knowledge Sharing, American Accounting Association, 26(2), pp. 71-91.

Spender J. C. (1996). Making Knowledge the Basis of a Dynamic Theory of the Firm, Strategic Management Journal, 17, pp. 45-62.
Stein M., Galliers R. D., Markus M. L. (2013). Towards an Understanding of Identity and Technology in the Workspace, Journal of Information Technology, 28, pp. 167-182.
Stein M., Newell S., Wagner E. L., Galliers R. D. (2012). Continued Use of IT: An Emotional Choice, ICIS 2012, paper 6.
Trkman P., Desouza K. C. (2012). Knowledge Risks in Organizational Networks: An Exploratory Framework, Journal of Strategic Information Systems, 21(1), pp. 1-17.
Tsoukas H., Vladimirou E. 2001. What is Organizational Knowledge? Journal of Management Studies, 38(7), pp. 973-993.
Venturini, T., and Latour, B. (2010). The Social Fabric: Digital Traces and Quali-quantitative Methods, in Proceedings of Future En Seine 2009: The Digital Future of the City, Digital, C. (ed.), Paris, France, pp. 30-15.
Von Krogh G. (2012). How does Social Software Change Knowledge Management? Toward a Strategic Research Agenda, Journal of Strategic Information Systems, 21(2), pp. 154-164.
Whelan E. (2007). Exploring Knowledge Exchange in Electronic Networks of Practice, Journal of Information Technology, 22, pp. 5-12.
Whitman, G. (2011). The New Paternalism: Unraveling 'nudge'. Economic Affairs, 31, 4-4.
Yoo, Y. (2010). Computing in everyday life: A call for research on experiential computing. MIS Quarterly, 34(2), pp. 213-231.
Yuan Y. C., Zhao X., Liao Q., Chi C. (2013). The Use of Different Information and Communication Technologies to Support Knowledge Sharing in Organizations: From e-mail to Micro-blogging, Journal of the American Society for Information Science and Technology, 64(8), pp. 1659-1670.
Wasserman S. 1994. Social Network Analysis: Methods and Applications, Cambridge University Press, Cambridge, MA.
Zuboff S. 1984. In the Age of Smart Machine: the future of work and power. NY: Basic Books