The Socio-technical Impact of the Internet of Things: An Exploratory Mixed Methods Research

Albert Boonstra[1][a] and Dustin A. Wiktor-Steffens[1,2][b]
[1]*Faculty of Economics and Business, University of Groningen, Nettelbosje 2, Groningen, The Netherlands*
[2]*School of Economics, Fudan University, 600 Guoquan Road, Shanghai, China*

Keywords: Internet of Things, Socio-technical Systems, Intentionality, Materiality.

Abstract: This study explores how the Internet of Things (IoT) impacts the socio-technical system of organizations. The paper adopts a mixed methods research with a qualitatively driven approach. Data from 21 interviews with experts in the field of IoT and an online survey with 123 IoT professionals were analyzed. Leonardi's Socio-Technical System Model (2012) was applied as a lens to examine how IoT influences the organizations' social subsystem and how that, in turn, affects both the materiality of IoT and users' intentionality in the technical subsystem. The results suggest transformed roles, potentially flattened hierarchies, decreased privacy, and increased transparency to be the main effects. While apparent changes in the social subsystem cause perceived threats that strongly influence users' intentionality, they do not certainly affect IoT's materiality. Noteworthy, however, is that irreplaceable users reportedly have the leverage to enforce changes to IoT's materiality.

1 INTRODUCTION

The physical world, as we know it, merges more and more with its digital counterpart. The Internet of Things (IoT) is driving this transformation we observe, by raising data collection to an unprecedented level. Emerging data that might drastically change the work of people in many organizations.

The International Data Corporation (IDC) forecasts the number of Internet-connected devices will increase from 30 billion in 2020 to 41.6 billion by 2025 – excluding general-purpose devices, such as smartphones, tablets, and PCs. In 2025, IoT devices will generate 79.4 zettabytes of data, providing unparalleled insight (MacGillivray & Reinsel, 2019). How IoT affects adopting organizations is still opaque. With this high-paced development in mind, one could perceive a sense of urgency, seeing the present unfamiliarity with IoT's socio-technical implications.

On the one hand, technological advancements, potential applications, and estimated economic growth through IoT are extensively discussed in journal articles, business reports, and news media. On the other hand, sufficient knowledge about the impact on people that work with IoT in organizations seems hitherto to be missing from the academic debate. Literature bodies either focus on socio-technical systems, which incorporate a general perspective on people and technology in organizations, or they focus on IoT, addressing the technical design and economics (Madakam, Ramaswamy, & Tripathi, 2015). Separately, these streams exist abundantly, but, as to the authors' knowledge, research combining both perspectives has yet to be published, thus offering many opportunities for research questions at all levels to be explored and tested in today's business environment.

Gaining a holistic view of the interaction between technology and people is critical. Chua and Lam (2005) argue for the fatality to consider the technical aspects unilaterally. Even though technical requirements can be met, the appropriation can be unsuccessful if the technology does not receive enough ongoing support from its users. Hence, it is crucial for the effective use of technologies to incorporate social aspects. This standpoint is shared by Boos and Grote (2012) as well as Shin (2014), saying that understanding and considering the

[a] https://orcid.org/0000-0002-3565-0623
[b] https://orcid.org/0000-0001-5635-1588

Boonstra, A. and Wiktor-Steffens, D.
The Socio-technical Impact of the Internet of Things: An Exploratory Mixed Methods Research.
DOI: 10.5220/0009327101770188
In *Proceedings of the 5th International Conference on Internet of Things, Big Data and Security (IoTBDS 2020)*, pages 177-188
ISBN: 978-989-758-426-8

interplay between technology and people is a pivotal success factor. In effect, failing to address both aspects in a balanced fashion leads to higher risks that technology implementations will not be used to their full potential or even remain without success.

IoT's social impact should not be left ignored (Shin & Jung, 2012). The current and little interdisciplinary academic discussion leaves us with the realization that some aspects of the socio-technical lens are not sufficiently explored and that the contemporary relevance of the topic allows for novel research questions. Using Leonardi's Socio-Technical System Model (2012) as a lens, this study aims to explore how IoT in the technical subsystem impacts the social subsystem and vice versa (see Figure 1). Through the presented model, the preliminary research question can be split into the following three research questions (RQ): RQ I addresses IoT's impact on the social subsystem, RQ II assesses the impact of changes in the social system on intentionality, and RQ III pays attention to the impact of changes in the social system on IoT's materiality (compare Figure 1).

2 LITERATURE REVIEW

Several academics agree that IoT is a collection of devices equipped with numerous types of sensors that are constantly connected via the Internet. These interconnected things collect and deliver precise data from the physical world without direct human involvement (e.g., Al-Fuqaha, Guizani, Mohammadi, Aledhari, and Ayyash (2015); Atzori, Iera, and Morabito (2017); Madakam et al. (2015).

The network of connected devices that continuously measures the environment with sensors generates large amounts of data. Enabled by a semantic layer, the technology transforms data into relevant information that holds meaning to the user. The automated collection of data in an unparalleled quantity constitutes the central affordance of IoT (Ouaddah, Mousannif, Abou Elkalam, & Ait Ouahman, 2017; Shi, Li, Zhu, & Ning, 2018). Affordances are all qualities of a technology that define its possible uses (Majchrzak & Markus, 2013; Volkoff & Strong, 2013).

Socio-technical system theory helps to analyze the organizational interplay between technology and people, especially how the affordance influences employees in their work environment. Because of the reciprocal relationship, socio-technical systems take both the technological and the social perspective into consideration. Paul Leonardi's (2012) model is especially suitable to observe IoT through the lens of the socio-technical system theory, as it incorporates the mutual shaping of technology and people and has not yet been used to analyze IoT. Moreover, it distinguishes the interrelatedness of the two perspectives, namely the *social subsystem* and the *technical subsystem*, in three main impacts; these serve as the basis to formulate the research questions (see center arrows in Figure 1).

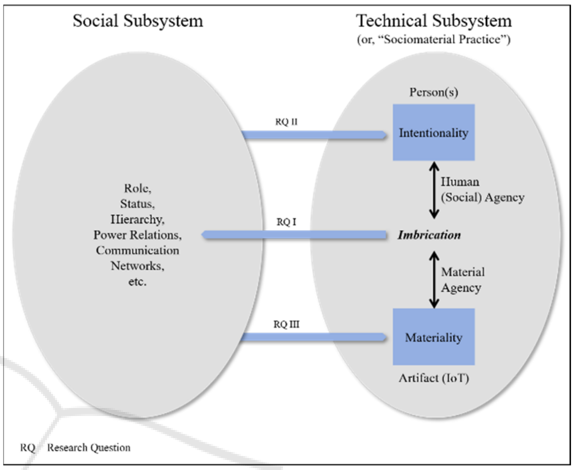

Figure 1: Socio-Technical System Model (Leonardi, 2012).

Leonardi describes a socio-technical system consisting of a *social subsystem* and a *technical subsystem* (Figure 1). The *social subsystem* is essentially a coherent whole that is formed by existing interrelationships between individuals within the organization. Generally, people that interact and work together build a stand-alone *social subsystem* within a group or organization. Defined by the relationships among the people in the *social subsystem*, it is influenced by various aspects like their abilities, power, assumptions and beliefs, knowledge, experience with and expectations about technology, as well as its affordances and constraints (Orlikowski & Gash, 1994).

The *technical subsystem* includes both the *person* and the *artifact*. The *artifact* refers to the technology as a non-human entity. It has its own *materiality*, which is the set-up of physical and digital materials in particular forms that matter to the user. Those properties of the *artifact* do not change, by themselves, across differences in time and context. *Materiality* produces the affordances and constraints of an *artifact* that are activated through *intentionality* (Leonardi & Barley, 2008).

Whereas *artifacts* have *materiality*, *persons* have *intentionality*, which expresses the desired outcome they have in mind. When users approach *artifacts* with *materiality*, they form particular goals or *human agency*. The coordination of multiple *human agencies* constitutes a *social agency* (Leonardi, 2012).

A central aspect of the interconnectedness is that the users' *intentionality* is subject to influencing factors in the *social subsystem*. To a large extent, users formulate their goals and decide in which ways they will proceed using the technology based on their perception of its possibilities and limitations. Their opinion about the technology is a result of the sensemaking process in the *social subsystem*. Thus, users have considerable influence on the degree to which technology affects their working environment.

To accomplish their intentions, people choose to use certain elements of the *artifact's materiality* at a given time. The *artifact's materiality* acts by users activating *material agency*, meaning they approach *materiality* with intentions. Hence, while *materiality* refers to properties of the object, *material agency* refers to the way the object acts when humans provoke it. A clear distinction is necessary because *materiality* is rather stable over time, but *material agency* frequently changes, depending on who is making sense of the *materiality* and which intentions this user has. The *social agency* is partly shaped in response to the *material agency* of all users in the system and how they perceive each other's intentions. The *material agency* would not exist without users' intentions to use the technology (Leonardi, 2012; Wagner, Newell, & Piccoli, 2010).

The *social* and *material agencies* are unlike each other but create a mutual new structure when both come together. Leonardi (2012) uses the term *imbrication* to explain this occurrence; the agencies become *imbricated* in the space of practice. In other words, individuals make use of the technology. As a matter of fact, *imbrication* is the actualization of the technologies' affordances. The study shows that specific *imbrications* cause changes in the *social subsystem*, such as in *roles, status,* and *hierarchies*. Transformations in these abstract formulations can form new future patterns of *imbrication*. Vice versa, these transformations can cause changes in the a*rtifact's materiality* and *person's intentionality*.

3 METHODOLOGY

Due to the underrepresentation of a holistic approach in research, this study is constructed using a qualitatively driven mixed methods design (Saunders, Lewis, & Thornhill, 2016). First, semi-structured expert interviews were conducted to identify and explain emerging phenomena. Based on the identified core aspects that emerged from the in-depth interviews, a questionnaire was designed and carried out to allow increased generalizability and triangulation. The quantitative results from the survey helped to create a clearer picture of the qualitative interviews. The qualitative analysis is dominant due to the need to create an initial understanding and provide the basis to generate theory. Results were compared across both the qualitative and quantitative data collection. Ultimately, generated insight was superimposed onto the presented model to derive conclusions (Eisenhardt, 1989).

3.1 Qualitative Part

For this study, the primary method is qualitative. Semi-structured expert interviews with limited access to documents were used to collect data as the topic's novelty gave reason to assume a lack of experience with IoT of most organizations and employees. A vastly distributed sample led to conducting interviews via phone with an average duration of 50 minutes. Each interviewee agreed to audio recordings for subsequent transcripts. One pretest call with feedback was performed to identify logical inconsistencies and unclear formulations. After transcribing all interviews, the computer program Atlas.ti was used to create and categorize codes. The coding of transcript included a balance of deductive and inductive codes to ensure theoretical and emerging aspects. The data was analyzed across experts.

The sample consists of 21 experts from business and academia from the US, China, India, Germany, the Netherlands, UK, Spain, and Sweden. All selected participants are responsible for, or knowledgeable of, the implementation and development of IoT. 90% are in leading positions or have notable decision-making power and staff responsibility. The represented organizations fall into the following roles: (1) IoT solution provider with additional services for their platforms and other use cases (43%), (2) management consulting firms with dedicated IoT practices (38%), (3) independent IoT research institutions (10%), (4) research and consulting firms (5%), and (5) internal IoT research and development (5%).

3.2 Quantitative Part

An online survey is the quantitative and thus secondary part of the mixed methods approach. It was designed to test the reliability of the expert interviews and to provide more generalizable results. The questionnaire was based on the research questions and propositions derived from qualitative expert interviews. Respondents (R) were mainly asked to evaluate eleven statements along the research questions on a 5-item Likert scale ranging from "strongly agree" to "strongly disagree." The results were used to support the insight generated through the primary interviews.

The response rate was 17.6% (N = 168). After scrutinizing for incomplete responses, unsuitable professions, and multivariate outliers, a sample of N = 123 remained. On average, respondents had eight years of experience in the field of IoT (M = 8.03, SD = 6.73). The majority reported being direct users of IoT applications (64.2%). Only 3.3% work for the government. Most participants work at organizations with over 10,000 employees (33.3%), with 1-4 employees (29.3%), and with 50-499 employees (18.7%)[2]. Their location is in Europe (37,4%), North America (27.6%), Asia (24.4%), South America (4.1%), the Middle East (4.1%), and in Oceania (2.4%).

4 RESULTS

4.1 Impact on Social Subsystem (RQ I)

The newly gained access to massive amounts of data supposedly is the main driver for changes in the social subsystem. The expert interviews confirm the central affordance of IoT: *"All of a sudden, you are able to read an incredible amount of sensor data, that really triggers the change" (R4, personal communication, 2018-04-30).* In addition, the interviews suggest that four dominant aspects in the social subsystem are affected by the abovementioned information flow. Each aspect will be considered below.

4.1.1 Transformed Role

Transformed roles are evident since aspects related to changes in employees' roles are touched upon during all primary interviews. Besides, the secondary survey demonstrates a high degree of agreement among the sample, as Figure 2 shows:

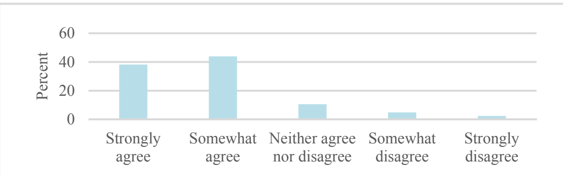

Figure 2: IoT Influences Roles in the Social System.

By influencing tasks and their required skills, IoT influences employees' roles in many facets. The experts imply that these shifts in demands associated with a particular role are likely to be disrupted in the age of IoT. Therefore, IoT questions the current roles of employees: *"Jobs […]; job profiles […and], qualifications are changing. Also important is the question, which work I will still be able to perform with my current set of qualifications and also which qualifications are required due to new technologies. That is a point that surely influences the whole social system" (R9, personal communication, 2018-05-08).*

After categorizing all codes contributing to the transformation of roles, the following four prevail. (1) *Gravitation towards an intellectual and digital role*: *"It will be essential whether they have an IT background or whether they manage to obtain that crucial knowledge" (R16, personal communication, 2018-11-21)*. (2) *Increased focus on core tasks*: *"Yet, you could provide a way to get rid of some of that administrative, nonvalue-added activities and let them do what they are trained to do" (R4, personal communication, 2018-04-30).* (3) *Upskilling workforce*: *"[IoT] demands employees to educate themselves further, both the textual and technical related competencies." (R3, personal communication, 2018-05-02)*. Lastly, (4) *redeployment of workforce into new role*: "*These employees who used to work as crane operators will be promoted to the supervisory level" (R16, personal communication, 2018-11-21)*.

4.1.2 Flattened Hierarchy

The primary interviews suggest that IoT implementations influence the hierarchy as a part of the social subsystem. More specifically, interviews imply the potential to flatten hierarchies, e.g.: *"When you deploy technologies like IoT that can have a side effect that flattens organizational hierarchies" (R12, personal communication, 2018-05-01).* The secondary survey supports this (see Figure 3) with 12% strongly agreeing and 41% somewhat agreeing. Factors causing flattened hierarchies were grouped into three categories: (1) *Gained accessibility of information*: E.g. *"[…] information come together at the top of the hierarchy. IoT could make it possible to distribute that information more, and that could result in a flatter hierarchy" (R8, personal communication, 2018-05-04).* (2) *Altering power relations*: *"[…] the gap between hierarchical levels could become smaller" (R8, personal*

[2] 6.5% with 500-999 employees, 6.5% with 5000-9999 employees, and 5.7% with 1000-4999 employees.

communication, 2018-05-04). And (3) the *restructuring through redundancy*: *[…I]nformation processing jobs go away. Simply because you have technology that learns those jobs" (R12, personal communication, 2018-05-01).*

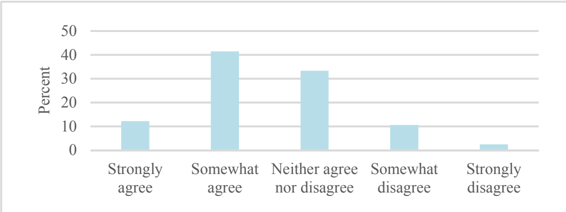

Figure 3: IoT Flattens Hierarchies.

4.1.3 Decreased Privacy

An IoT-enabled working environment almost inevitably observes employees and collects data about them, which are potentially accessible to others.

Losing privacy means being uninformed about ongoing observations and lacking the freedom to reject these (Sarwar, Yongchareon, & Yu, 2018). Decreased privacy raises concerns that seem to impact the social subsystem strongly. Emerging concerns are also widely recognized in the provided documents and the secondary survey (Figure 4) with 37% strongly agreeing and 38% somewhat agreeing.

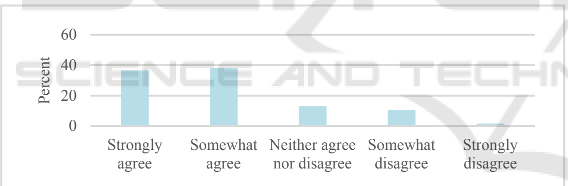

Figure 4: The Extensive Data Collection through IoT Triggers Privacy Concerns among Employees.

Privacy is potentially a trade-off for improved organizational efficiency, as organizations incorporate more monitoring to increase their measurable profitability. Hence, this may be an indicator that profit-driven organizations will keep touching upon these concerns: *"Because surveillance […] is an outgrowth of efficiency and bureaucratic evolution. The highly monitored nature of the world that we are beginning to experience is a natural outgrowth of a variety of socio-technical trends" (R6, personal communication, 2018-05-02).*

The protection of privacy is a requirement for employees to develop trust, enabling them to harness IoT's benefits: *"[…] you start with trust by doing these proper [privacy] reviews and implementing proper safeguards and then after that, hopefully, the employees do see the benefits and the value" (R4, personal communication, 2018-04-30).* Policies, e.g., the European General Data Protection Regulation (GDPR), limit the neglect of privacy in the course of efficiency gains. Though, there are significant national differences, having a decisive influence on risks related to privacy: *"It may be totally different in Germany, Austria, Switzerland, and Europe, compared to the United States, China, and Africa" (R1, personal communication, 2018-05-04).* Additionally, the presence and power of labor unions representing the workforce diverge across different nations.

Lastly, one expert mentions the possible occurrence of splits in the social subsystem, reporting that *"in the worst case, it will cleave the social system in two."* The trigger of faultlines may be the employees' tolerance towards privacy concerns: *"On one hand [there are] people who don't 'care' and make maximum use of IoT and take advantage of it. They also agree to pay the price in form of data. […] On the other hand, there will be people who try to evade IoT completely" (R10, personal communication, 2018-05-08).* A Faultline is a gap that splits a group into at least two subgroups, caused by certain attributes that each subgroup identifies with (Meyer & Schermuly, 2012). The secondary survey results support this phenomenon as the majority of respondents (68.3%) agree that "IoT causes contrasting opinions about privacy, which create faultlines."

4.1.4 Increased Transparency

Based on the experts, transparency is about the continuous accessibility of performance measurement. Integrated sensors enable organizations to monitor employees' actions and decisions constantly. For instance, a *"[…] truck driver who sits in such a connected truck, of course, is fully monitorable and it is always clear where he is, when he drives, when does he stand, how much fuel does he consume, how much do his colleagues consume, and so on" (R1, personal communication, 2018-05-04).*

IoT-enabled performance measurements do not seem to resonate positively with employees: *"Actually, I hardly know any worker who is interested in his work being measured" (R14, personal communication, 2018-05-07).* The primary interviews and secondary survey support that increasing transparency seems to create a threat of losing one's autonomy (see Figure 5) with 13.0% strongly agreeing and 41.5% somewhat agreeing.

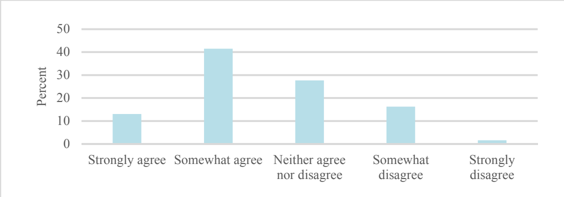

Figure 5: IoT-Enabled Performance Metrics About Employees Decrease Their Perceived Autonomy.

The interviews reveal that two factors can influence the perception of increased transparency positively. Firstly, educating users regarding the provided advantages that come with more transparency. A reoccurring example from the interviews is improved safety, e.g., through IoT-enabled trucks preventing accidents. Secondly, informing users about how gathered insight is utilized might change the perception from negative to positive: *"When it is ambiguous, when they do not know what they are being monitored for, it is definitely negative. But, if, if the company is telling them upfront that they are not trying to pin-point a particular driver or put a penalty on a particular person, but, overall trends which all the trucks combined generate and hence they know this or that route is better, where they should refuel the vehicles. All these kinds of definitions come out, and they know that they will not be individually monitored, then, I think, it becomes positive" (R17, personal communication, 2019-02-12).*

4.2 Impact on Intentionality (RQ II)

The gathered interview data show that employees' intentionality conceivably alters due to changes in the social subsystem: *"Yes, there will probably be behavioral changes. I would be honestly surprised if it did not […]" (R1, personal communication, 2018-05-04).*

4.2.1 Expression of Changed Intentionality

The primary interview data suggest that changes related to intentionality appear to surface in three forms of negative behavior: (1) *Reduced willingness to use IoT*: *"[…] I would say, yes, […] he either avoids using or avoids using parts of the technology […]" (R9, personal communication, 2018-05-08).* (2) *Application of workarounds*: *"[T]he user could try to use a workaround" (R15, personal communication, 2018-04-29).* (3) *Resistance towards the implementation of IoT solutions*. Especially privacy concerns were mentioned as a possible cause for threats that result in resistance: *"You feel like big brother is watching. I think privacy is one of the elements that would drive the resistance and especially in industrial Europe because some of the other regions are far less concerned about privacy" (R4, personal communication, 2018-04-30).*

4.2.2 Causes for Changed Intentionality

The secondary survey results support that the four previously introduced social aspects in chapter 4.1 might impact intentionality. The survey respondents ranked the four social aspects in order of their potential to provoke resistant behavior: first, privacy (M = 1.62, SD = .944), second, transparency (M = 2.69, SD = 1.094), third, hierarchy (M = 2.81, SD = .977), and fourth, role (M = 3.09, SD = 1.116).

While the social aspects constitute the major influence of IoT on the social subsystem, the primary interviews infer these changes to translate into two factors that impact employees' intentionality: (1) *Perceived threats*. Employees do not necessarily fear the technology but what comes along with it. They *"[…] can be quite fearsome […]. That doesn't necessarily have to be with regards to the quality of the hardware and the software […] but it can be seen as a certain threat to their job, changes in the hierarchy, and that creates that he might not adopt new technologies or refuses them" (R8, personal communication, 2018-05-04).* Therefore, it appears that changes in the social subsystem can cause threats, potentially altering employees' intentionality. These findings are backed by the survey where most respondents (58.4%) agree that perceived threats resulting from changes in the social system alter users' intention to deploy IoT solutions (Figure 6).

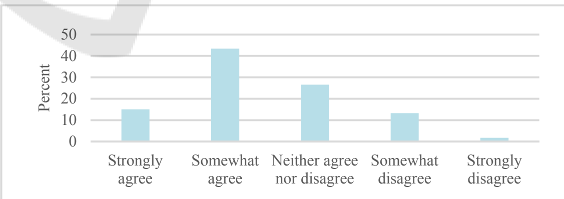

Figure 6: Perceived Threats Resulting from Changes in the Social System Alter Users' Intention to Deploy IoT Solutions.

(2) *Perceived Opportunities*. It seems to be crucial whether employees are aware of their individual benefits. Therefore, employees would, e.g., neglect the technology when the added value is invisible or unclear to them. The individual benefits should clearly outweigh the costs (represented by the potential threat): *"If they see value in what's on offer, then they'll become comfortable with it over time;*

They need to see the benefits, […] it's a trade-off, right? It's about how you articulate the value" (R12, personal communication, 2018-05-01).

The interviews suggest that organizations already try to avert unfavorable intentionality by involving employees right from the start. Thus, in advance to the implementation, perceived threats and employees' awareness of individual benefits are addressed early in the process. Organizations consider both the human perspective as well as economic efficiency to be crucial for proper IoT implementations: *"Companies realized that they must make it right in the beginning to avoid unpredictable behavior of employees and to avoid wasting money" (R12, personal communication, 2018-05-01).*

4.3 Impact on IoT's Materiality (RQ III)

The interviews imply materiality to be less influenceable than intentionality once IoT is introduced. The experts' tendency is that organizations do not consider adjusting the materiality due to changes in the social subsystem once the technical integration is completed: *"Changing the technology, I consider difficult, changing the use of technology, I consider absolutely feasible." (R9, personal communication, 2018-05-08).* Substantial adjustments to IoT's materiality are unlikely for three reasons:

(1) *Exploitation of performance advantages.* The expert states that *"if the output is right, the company will not change the technology, even if the employee is dissatisfied or there are other negative effects in the social system."* IoT solutions will remain the same unless effects in the social subsystem significantly impair the performance. E.g. *"[…] if the output is not right, if the employee refuses or develops a workaround that is not legit anymore, then the company would be forced to adjust" (R15, personal communication, 2018-04-29).*

(2) *The necessity to stay competitive* is driving the application of IoT solutions: *"From a corporate perspective, dealing with IoT is relevant to competition."* The advantages arise, for instance, from the following: *"If I am faster in the future, if I reduce machine errors if I can predict downtimes of the machines and thus prevent them. It's important for the company to do that" (R3, personal communication, 2018-05-02).* Therefore, adjustments of the materiality, which are limiting the potential exploitation of the capabilities may be improbable. Especially, as IoT is a means to become future proof: *"Personally, I don't think that these social aspects can change the architecture. […] Because the company that decided in favor of the IoT solution. I mean, they are investing in the future" (R16, personal communication, 2018-11-21).* Evaluating IoT as an essential element on the digital agenda is also reflected by the survey results: 46% of the respondents think that IoT's importance for firm performance is somewhat above average, and 39.8% even think it is far above average.

(3) *Problem to reverse the integration of technological elements of IoT.* On the one hand, there is the view that adjustments are out of the question since organizations have a set of motives for not adjusting IoT's materiality and, therefore, the disadvantages prevail. 14% of the experts argue that one cannot just make technology disappear: *"It cannot be ruled out that the properties of IoT solutions will be changed, but basically, of course, it is usually the case that once a technology is integrated, it is difficult to restrain it again" (R1, personal communication, 2018-05-04).* On the other hand, however, experts emphasize the general magnitude of the social aspects related to IoT. Their responses to the latter are all similar to the statement: *"For me, that means that I personally would even put the social aspects at the heart of an IoT development" (R15, personal communication, 2018-04-29).* Only 10% of the experts can envision organizations adjusting IoT's materiality: *"I guess, in any scenario […] you have to be accommodating to two things, to your bottom-line, but also to your staff and their feelings. So, you have to take both into account […]. I can see that there are changes made" (R13, personal communication, 2018-05-10).* In line with this statement, the secondary survey shows that 46.9% disagreed with the statement that the technical design of IoT solutions remains unchanged despite changes in the social system, while only 33.6% agreed. A potential explanation for this discrepancy might lie in the stages in time in which social aspects are incorporated. Organizations address social issues already before and during the implementation process of IoT, whereas "changing" materiality implies a post-implementation stage. The experts unanimously describe that *"[…] especially in the field of IoT […it] is too costly if you first develop something and then check the feasibility or user acceptance, etc" (R15, personal communication, 2018-04-29).*

Whether or not organizations adjust the technology's materiality depends on a moderating effect of employees' leverage over the organization. Analyzing the interview data, several leverage-creating attributes were accumulated: expertise, flexibility in mobility, hierarchical level, and unique skill set. Vice versa, the employer has attributes to exert leverage over the respective employee with access to qualified workforce and flexibility in mobility. Survey respondents generally agree that employees who possess power within the organization have a noteworthy influence on IoT's materiality (69% agree, and 16.9% disagree). Given that both employees and employers appear to have leverage, they may have to be weighed against each other to assess whether potential changes in IoT's materiality need to be addressed or can be suppressed.

5 DISCUSSION

5.1 Answering the Research Questions

The primary expert interviews and the secondary survey results help to explore the impacts of IoT within Leonardi's Model (2012). The adjusted model in Figure 7 presents the discussion's outcomes.

5.1.1 Impact on Social Subsystem (RQ I)

The results suggest the following four ways how IoT impacts the social subsystem:

(1) *Transformed Role.* The results suggest that employees' roles will change as IoT enables increasing automation and massive information enrichment. In line with the literature, the findings advise that constant education is crucial to maintaining a valuable role within the organization (Bresnahan, Brynjolfsson, & Hitt, 2002). Computerization, primarily driven by data acquirement via sensors, increases the demand for highly educated and creatively thinking roles (Frey & Osborne, 2017). Therefore, employees must be prepared to adapt their roles faster in an IoT accelerated environment.

(2) *Flattened Hierarchy*. This research proposes that IoT flattens organizational hierarchies when information is distributed equally and across all levels. Information is a source of power (Pettigrew, 2016). When information is available at all levels, it is most-likely to re-allocate decision-making powers and flatten hierarchical patterns (Dobrajska, Billinger, & Karim, 2015). Moreover, IoT can be responsible for technological unemployment (Brynjolfsson & McAfee, 2014).

(3) *Decreased Privacy*. Privacy issues have a substantial impact on employees' well-being. To a degree, security matters can justify employees' location tracking or video surveillance. Generally, privacy concerns among employees cause decreased acceptance of IoT solutions. Bélanger and Crossler (2011) support that privacy concerns reduce the intention to use information technologies. Their study implies four dimensions that cause uneasiness of employees: (1) nontransparent collection of data, (2) unauthorized secondary use of data, (3) improper access to data, and (4) errors in data. The results even reveal that privacy concerns can be considered as a cause for passive to active forms of resistance (Chang, Liu, & Lin, 2015). Also, the occurrence of faultlines provoked by privacy is possible, separating the social subsystem into subgroups ranging from being concerned with privacy issues to not being concerned with them at all. These subgroups may increasingly work against each other, harming the organization (Meyer & Schermuly, 2012).

(4) *Increased Transparency*. Research of Levy (2018) about truck drivers in IoT-supported vehicles comes to a similar conclusion that transparent performance metrics likely negatively affect job satisfaction. The underlying reasons may be the felt loss of leeway and decision freedom. Continuous controllability through sensors takes away employees' autonomy. As a consequence, diminished autonomy leads to lower job satisfaction and can cause burnout symptoms (Arches, 1991). On the contrary, it was also reported that increased transparency generates data that can facilitate fairness by providing additional proof, e.g., in the case of truck accidents.

5.1.2 Impact on Intentionality (RQ II)

The abovementioned four social aspects identified in this research, do not directly impact users' intentionality. Instead, transformed roles, flattened hierarchies, decreased privacy, and increased transparency, constitute changes as these new circumstances diverge from the incumbent status quo. These changes cause perceived threats that ultimately seem to result in alterations in intentionality. This is in line with Lapointe and Rivard (2005), describing that it is the object of change that interacts with initial conditions and not the technology or a specific aspect in the social system itself that triggers perceived threats.

In the case of technology adaptation, perceived opportunities lead to the exploitation of a given technology or even the exploration to innovate. On the contrary, perceived threats cause an exploration to revert or even avoidance of the technology (Bala & Venkatesh, 2016). This interplay is in sync with the change equation, describing that the benefit of and need for change must outweigh the costs of change (Beckhard, 1975; Dannemiller & Jacobs, 2016). This notion is also explained by the equity theory in social sciences, describing the assessment of gain and loss of changes (Joshi, 1991).

Hence, perceived opportunities compromise the moderating effect of perceived threats on intentionality (see Figure 7). The study suggests that mainly, the four identified social aspects cause threats that trigger a range of reactions away from neutral behavior to passive or active resistance (van Offenbeek, Boonstra, & Seo, 2013). Therefore, organizations must ensure to incorporate these social aspects to reinforce successful IoT implementations (Bersin, Mariani, & Monahan, 2016; Jones, Derasse, Chitale, & Negri, 2016).

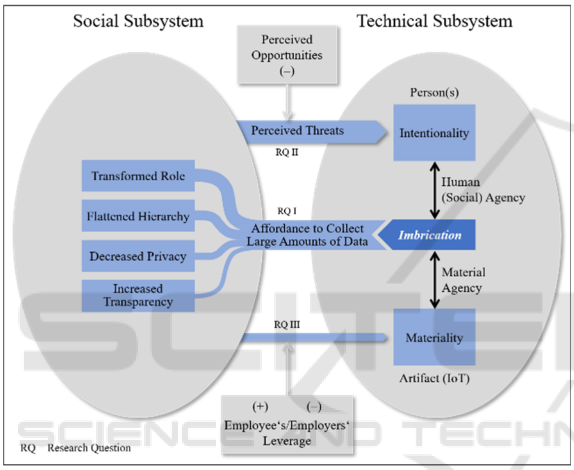

Figure 7: Adjusted Socio-Technical System Model.

5.1.3 Impact on IoT's Materiality (RQ III)

The conducted research infers that it is indistinct whether organizations adjust IoT's materiality in response to changes in the social subsystem. On one side, the findings show that the immense investments of IoT implementations hamper organizations to leave their planned course of action, even though people in the social subsystem express their aversion. Exploring why organizations do not reverse technological implementations while facing substantial headwinds, Keil, Truex, and Mixon (1995) propose two main factors, the level of costs and the level of project completion. Both aspects determine the influenceability of materiality. The higher the costs and further the progress of implementation, the less likely adjustments appear. In their consideration, costs were even more significant than project progress.

In fact, multiple sources confirm that IoT is considered to be exceptionally cost-intensive compared to other technologies. Thus, organizations are compelled to assess each challenge thoroughly and plan, design, and deploy all aspects with the highest diligence (Lee & Lee, 2015; Niyato, Lu, Wang, Kim, & Han, 2016). The necessity to *"do it right the first time" (R12, personal communication, 2018-05-01)* reflects the necessity of great efforts in change management during the implementation. It is too costly to adjust materiality because of adverse responses in hindsight. Nevertheless, the survey results also point at a perceived high likelihood that organizations do consider adjustments of IoT's technical design due to social changes. However, some employees have distinctive qualities, such as a unique skill set, which creates an overall exception to enforcing adjustments of materiality. Their leverage makes organizations incapable of ignoring their criticism unless they exert leverage themselves through, e.g., their access to a large selection of qualified applicants. The forces of both parties appear to have a moderating effect on how changes in the social subsystem influence the materiality in the technical subsystem (compare Figure 7).

5.2 Theoretical Contributions

The study is the first to bring a degree of clarity to the way IoT affects the employee in the social subsystem by applying the theory of Leonardi (2012). The reported main effects open the hitherto black box of social implications provoked by IoT (Shin & Jung, 2012). Moreover, it is the first study to explore how effects in the social subsystem influence users' intentionality.

The findings confirm the idea that it is an object of resistance instead of specific artifacts or elements in the socio-technical system that creates perceived threats. Employees assess the costs and benefits of the disruption of their initial state for an upcoming change. A prevailing perception of a threat will provoke resistant behaviors, spanning from avoidance, over applying workarounds, to active resistance (Lapointe & Rivard, 2005).

The study addressed the influence of social effects on IoT's materiality, unveiling indistinct results. There is ambiguous evidence whether organizations would adjust the technology due to changes in the social subsystem. Several incentives keep organizations from adjusting their IoT solutions. Among them are, for example, the tremendous costs that come along with an IoT implementation and the necessity to incorporate IoT use cases to stay competitive (Keil et al., 1995). However, the results show a moderating effect of both employees' and employers' leverage over each other. Consequently, a moderator was added to the model (Figure 7) to imply the evaluation of, for instance, the employees' leverage due to a unique skill set versus the employers' extensive access to skilled people.

5.3 Practical Implications

Derived from IoT expert interviews, the recommendations' suitability is neither limited to IoT nor should they be understood as exhaustive. First, the results determine the four core aspects that ought to be monitored with close attention on the journey to IoT appropriation. Ideally, before, during, and after the implementation to detect even slight irregularities over time and avoid perceived threats.

Second, when perceived threats endanger users' intentionality, the study suggests presenting perceived opportunities to be an effective counteraction. Accordingly, benefits for involved users should be put at the center of the discussion.

5.4 Research Limitations

Due to IoT's arguable novelty and (so far) limited distribution, expert interviews were preferred over interviews with directly affected employees. While this method allowed comprehensive insight into IoT in the socio-technical system, the observations are more abstract. The majority of survey respondents, however, reported already being direct users of IoT.

The in-depth analysis of mechanisms had to be neglected due to the variety of specialist knowledge among the interviewees. Gathering various examples from different fields was, nevertheless, more valuable for a universal understanding.

40% of interviewees are German, which can bias the results because of the geographical commonalities such as strong privacy regulations and labor unions.

The supplementary survey was distributed via professional networks. While reducing the chance of contextual misunderstandings, the approach inherits a risk of selection bias and false individual portrayal.

Although IoT can be explicitly described, its use cases often blur with other technologies. Since it is the infrastructure and enabler for several themes, it is challenging to match cause and effect to a distinctive technology. Therefore, the reader ought to be reminded that IoT operates among other technologies that influence findings reciprocally.

5.5 Suggestions for Further Research

This study contributes to laying the foundation for future research exploring detailed mechanisms through, e.g., a specific IoT application in an empirical setting. Thus, the presented adapted model (Figure 7) can be utilized for case studies to verify its reliability.

Furthermore, in the light of practical relevance, future research should investigate strategies to counteract disturbances in the socio-technical system related to IoT.

6 CONCLUSIONS

Numerous scholars and reports (e.g., Shi et al., 2018; Bhatia et al., 2017; Bersin et al., 2016) emphasize the magnitude of IoT as it is a driving force for the digital revolution. Looking at the current IoT research, the predominant focus on technology and business issues becomes apparent. Consequently, the social component does not receive the attention it deserves, considering its importance after implementation.

At question is in what way IoT in the organization's technical subsystem impacts the social subsystem and vice versa. The analysis shows that access to an unprecedented amount of data affects some aspects of the social subsystem more than others. These are transformed roles, flattened hierarchies, decreased privacy, and increased transparency. The findings indicate two moderating effects in the socio-technical system. Firstly, alterations in the social subsystem lead to perceived threats that negatively change users' intention to use IoT. However, perceived opportunities through IoT have a moderating effect as they weaken this relationship. Secondly, alterations in the social subsystem may have little impact on IoT's materiality due to, e.g., the necessity to remain competitive. Nonetheless, the relationship between social subsystem and materiality can be affected by the respective individuals and their unique characteristics; employees with arguably important attributes have leverage to reinforce the relationship, leading to more technical adjustments. Employers' leverage, however, can weaken the relationship.

This study aims to raise awareness of the social impact of IoT, in the hope that future research will shift its focus beyond technological and economic opportunities to a more human-oriented approach.

REFERENCES

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials*, *17*(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

Arches, J. (1991). Social Structure, Burnout, and Job Satisfaction. *Social Work*, 202–206. https://doi.org/10.1093/sw/36.3.202

Atzori, L., Iera, A., & Morabito, G. (2017). Understanding the Internet of Things: Definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks*, *56*, 122–140. https://doi.org/10.1016/j.adhoc.2016.12.004

Bala, H., & Venkatesh, V. (2016). Adaptation to Information Technology: A Holistic Nomological Network from Implementation to Job Outcomes. *Management Science*, *62*(1), 156-179. https://doi.org/10.1287/mnsc.2014.2111

Beckhard, R. (1975). Strategies for large system change. *Sloan Management Review*, *16*(2), 43–55.

Bélanger, F., & Crossler, R. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*(4), 1017–1042. https://doi.org/10.2307/41409971

Bersin, J., Mariani, J., & Monahan, K. (2016). *Will IoT Technology Bring us the Quantified Employee?* Retrieved from Deloitte website: https://www2.deloitte.com/content/dam/insights/us/articles/people-analytics-iot-human-resources/ER_3104_IoT_Human-capital_vFINAL.pdf

Bhatia, A., Hunke, N., Kalra, N., Rüßmann, M., Schmieg, F., & Yusuf, Z. (2017). *Winning in IoT: It's all about the business processes*. Boston, United States. Retrieved from The Boston Consulting Group (BCG) website: http://img-stg.bcg.com/BCG-Winning-IoT-Jan-2017_tcm9-161204.pdf

Boos, D., & Grote, G. (2012). Designing Controllable Accountabilities of Future Internet of Things Applications. *Scandinavian Journal of Information Systems*, *24*(1), 1–28. Retrieved from http://aisel.aisnet.org/sjis/vol24/iss1/1

Bresnahan, T. F., Brynjolfsson, E., & Hitt, L. M. (2002). Information Technology, Workplace Organization, and the Demand for Skilled Labor: Firm-Level Evidence. *The Quarterly Journal of Economics*, *117*(1), 339–376. https://doi.org/10.1162/003355302753399526

Brynjolfsson, E., & McAfee, A. (2014). *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies* (First Edition). New York: W. W. Norton & Company.

Chang, S. E., Liu, A. Y., & Lin, S. (2015). Exploring privacy and trust for employee monitoring. *Industrial Management & Data Systems*, *115*(1), 88–106. https://doi.org/10.1108/IMDS-07-2014-0197

Chua, A., & Lam, W. (2005). Why KM projects fail: A multi‐case analysis. *Journal of Knowledge Management*, *9*(3), 6–17. https://doi.org/10.1108/13673270510602737

Dannemiller, K. D., & Jacobs, R. W. (2016). Changing the Way Organizations Change: A Revolution of Common Sense. *The Journal of Applied Behavioral Science*, *28*(4), 480–498. https://doi.org/10.1177/0021886392284003

Dobrajska, M., Billinger, S., & Karim, S. (2015). Delegation Within Hierarchies: How Information Processing and Knowledge Characteristics Influence the Allocation of Formal and Real Decision Authority. *Organization Science*, *26*(3), 687–704. https://doi.org/10.1287/orsc.2014.0954

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *Academy of Management Review*, *14*(4), 532–550. https://doi.org/10.5465/AMR.1989.4308385

Frey, C. B., & Osborne, M. A. (2017). The future of employment: How susceptible are jobs to computerisation? *Technological Forecasting and Social Change*, *114*, 254–280. https://doi.org/10.1016/j.techfore.2016.08.019

Jones, A., Derasse, A., Chitale, A., & Negri, A. (2016). *Internet of Things: Visualise the Impact*. USA.

Joshi, K. (1991). A Model of Users' Perspective on Change: The Case of Information Systems Technology Implementation. *MIS Quarterly*, *15*(2), 229–242. https://doi.org/10.2307/249384

Keil, M., Truex, D. P., & Mixon, R. (1995). The effects of sunk cost and project completion on information technology project escalation. *IEEE Transactions on Engineering Management*, *42*(4), 372–381. https://doi.org/10.1109/17.482086

Lapointe, & Rivard (2005). A Multilevel Model of Resistance to Information Technology Implementation. *MIS Quarterly*, *29*(3), 461–491. https://doi.org/10.2307/25148692

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431–440. https://doi.org/10.1016/j.bushor.2015.03.008

Leonardi, P. M. (2012). Materiality, Sociomateriality, and Socio-Technical Systems: What Do These Terms Mean? How Are They Different? Do We Need Them? In P. M. Leonardi, B. A. Nardi, & J. Kallinikos (Eds.), *Materiality and Organizing* (pp. 25–48). Oxford University Press.

Leonardi, P. M., & Barley, S. R. (2008). Materiality and change: Challenges to building better theory about technology and organizing. *Information and Organization*, *18*(3), 159–176. https://doi.org/10.1016/j.infoandorg.2008.03.001

Levy, K. (2018, January). *Data Driven: Truckers and the New Workplace Surveillance.* Berkeley Sociology, Berkeley, United States. Retrieved from http://sociology.berkeley.edu/karen-levy-data-driven-truckers-and-new-workplace-surveillance

MacGillivray, C., & Reinsel, D. (2019). *Worldwide Global DataSphere IoT Device and Data Forecast, 2019–2023.*

Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications*, *03*(05), 164–173. https://doi.org/10.4236/jcc.2015.35021

Majchrzak, A., & Markus, L. (2013). Technology Affordances and Constraints in Management Information Systems. In E. H. Kessler (Ed.), *Encyclopedia of Management Theory* (pp. 832–835). 2455 Teller Road, Thousand Oaks, California 91320: SAGE Publications, Ltd.

Meyer, B., & Schermuly, C. C. (2012). When beliefs are not enough: Examining the interaction of diversity faultlines, task motivation, and diversity beliefs on team performance. *European Journal of Work and Organizational Psychology*, *21*(3), 456–487. https://doi.org/10.1080/1359432X.2011.560383

Niyato, D., Lu, X., Wang, P., Kim, D. I., & Han, Z. (2016). Economics of Internet of Things: An information market approach. *IEEE Wireless Communications*, *23*(4), 136–145. https://doi.org/10.1109/MWC.2016.7553037

Orlikowski, W. J., & Gash, D. C. (1994). Technological frames: Making sense of information technology in organizations. *ACM Transactions on Information Systems*, *12*(2), 174–207. https://doi.org/10.1145/196734.196745

Ouaddah, A., Mousannif, H., Abou Elkalam, A., & Ait Ouahman, A. (2017). Access control in the Internet of Things: Big challenges and new opportunities. *Computer Networks*, *112*, 237–262. https://doi.org/10.1016/j.comnet.2016.11.007

Pettigrew, A. M. (2016). Information Control as a Power Resource. *Sociology*, *6*(2), 187–204. https://doi.org/10.1177/003803857200600202

Sarwar, K., Yongchareon, S., & Yu, J. (2018). A Brief Survey on IoT Privacy: Taxonomy, Issues and Future Trends. In *Liu X. et al. (eds) Service-Oriented Computing – ICSOC 2018 Workshops*. Springer; Cham.

Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research Methods for Business Students* (7th ed.). Harlow, United Kingdom: Pearson.

Shi, F., Li, Q., Zhu, T., & Ning, H. (2018). A Survey of Data Semantization in Internet of Things. *Sensors (Basel, Switzerland)*, *18*(1), 313. https://doi.org/10.3390/s18010313

Shin, D. (2014). A socio-technical framework for Internet-of-Things design: A human-centered design for the Internet of Things. *Telematics and Informatics*, *31*(4), 519–531. https://doi.org/10.1016/j.tele.2014.02.003

Shin, D.-H., & Jung, J. (2012). Socio-technical analysis of Korea's broadband convergence network: Big plans, big projects, big prospects? *Telecommunications Policy*, *36*(7), 579–593. https://doi.org/10.1016/j.telpol.2012.03.003

Van Offenbeek, M., Boonstra, A., & Seo, D. (2013). Towards integrating acceptance and resistance research: Evidence from a telecare case study. *European Journal of Information Systems*, *22*(4), 434–454. https://doi.org/10.1057/ejis.2012.29

Volkoff, O., & Strong, D. M. (2013). Critical Realism and Affordances: Theorizing IT-Associated Organizational Change Processes. *MIS Quarterly*, *37*(3), 819–834. https://doi.org/10.25300/MISQ/2013/37.3.07

Wagner, E., Newell, S., & Piccoli, G. (2010). Understanding Project Survival in an ES Environment: A Sociomaterial Practice Perspective. *Journal of the Association for Information Systems*, *11*(5), 276–297. https://doi.org/10.17705/1jais.00227