The integrity challenge of the Internet-of-Things (IoT):on understanding its dark side

De Cremer, D., Nguyen, B., Simkin, L.

Original citation & hyperlink:
De Cremer, D, Nguyen, B & Simkin, L 2016, 'The integrity challenge of the Internet-of-Things (IoT):on understanding its dark side' Journal of Marketing Management, vol 33, no. 1-2, pp. 145-158. DOI: 10.1080/0267257X.2016.1247517
https://dx.doi.org/10.1080/0267257X.2016.1247517

DOI 10.1080/0267257X.2016.1247517
ISSN 0267-257X
ESSN 1472-1376

Publisher: Taylor & Francis

This is an Accepted Manuscript of an article published by Taylor & Francis in Journal of Marketing Management on 4 Nov 2016, available online:
http://www.tandfonline.com/ 10.1080/0267257X.2016.1247517

The Integrity Challenge of the Internet-of-Things (IoT): On Understanding its Dark Side

Professor David De Cremer, KPMG Professor of Management, Judge Business School, University of Cambridge, UK. Email: d.decremer@jbs.cam.ac.uk

Dr. Bang Nguyen, East China University of Science and Technology**,** 130 Meilong Road, Xuhui District, Shanghai 200237, China**.** Email: bang.london@gmail.com

Professor Lyndon Simkin, Coventry University, Centre for Business in Society, Coventry, UK. Email: ac0953@coventry.ac.uk

Abstract

Despite the overall positive feeling about Internet of Things' (IoT) development, a main risk involves the integrity of the system itself. This paper considers the influence of the IoT on marketing practices and addresses the overlooked area of the dark side of the IoT. Dysfunctional forms of IoT have been neglected as an area of research, so identifying the different types of IoT providers' dark side behaviours will assist in the development of an integrated approach to the IoT that will help to overcome or mitigate these dark side behaviours. Based on an extensive literature review, supplemented by expert insights drawn from the authors' study of the IoT, a framework is developed that classifies the varying IoT dark side behaviour types. The framework reveals eight forms of dark side behaviour that are grouped into four broad categories. This classification illustrates how different types of dark side behaviours are linked to key strategic IoT processes and also outlines how these dark side practices may be addressed by adopting a more strategic and integrity-oriented approach. We conclude that with the adoption of a more holistic approach to the IoT, dark side behaviours can be addressed and move in the direction of more effective marketing practices.

Keywords - Internet of Things, IoT relationship, IoT network, IoT dark side, IoT integrity

Introduction

The Internet-of-Things (IoT) is a network of interconnected devices, systems and services within the existing Internet infrastructure. The core of the IoT is that it allows for 'all things connected' in the communication between devices and objects, creating a more direct integration between the physical world and computer-based systems. By capturing and analysing the data that comes from the sensors at the endpoints of the connected objects, the IoT's value lies in its ability to track, measure and create 'smart' devices that bring considerable benefits to individuals, businesses and society (Nguyen and De Cremer, 2016). For example, integrating IoT into the health care system with wearable technology or implanted microchips, allows for hospitals to monitor patients' vital signs in real time. By tracking their vital signs, doctors can observe whether or not a more invasive and resource-demanding assessment is necessary. For businesses, the *industrial* IoT can be useful in many different categories, most notably, those related to asset tracking and inventory control, security, tracking of shipping, location and energy conservation, as well as building profiles of customers and suppliers. With extensive data tracking and measurement, a potential lies in predicting and subsequently automating logistical processes, resulting in a more expedient and effective value chain. The outcome is that operations work in a more efficient way with improved efficiency, accuracy and economic benefit.

Resources applied to such IoT initiatives are substantial and growing. For example, modest estimates suggest that there will be anywhere between 20 billion devices (Gartner, 2015) to 50 billion devices (WoodsideCap, 2015) that will be wirelessly connected to the IoT by 2020. On a more optimistic level, other estimates show that there will be over 50 billion connected devices by 2020 (NCTA, 2015). This explosion of connected devices ranges anything from smart phones, tablets and computers to toothbrushes, stovetops, cars and millions of other devices that now have IP addresses. According to Gartner (2015), many of

the IoT systems and technologies are expected to usher in automation in nearly all fields. McKinsey Group (2015) estimates that the IoT has a total potential economic impact of $3.9 trillion to $11.1 trillion a year by 2025. At the top end, that level of value would be equivalent to about 11% of the world's economy.

However, despite the overall positive feeling about the IoT's development, and while the IoT brings considerable benefits when it works, this is not at all guaranteed. In fact, many IoT practices manifest behaviour that damages or even destroys interfirm- and customer relationships. Indeed, as the IoT relies extensively on delivering information to businesses to capitalise on the data supplied, a problem of integrity may emerge. For example, Snyder (2015) notes that from our homes the Internet allows us to reach into the outside world, but it also allows the world to reach inside our homes. Such integrity problem poses a major challenge and needs further exploration.

In this present paper, we focus on the management of IoT activities that can damage customer relationships and the malicious practices that exploit customers deliberately, which include a focus on both dark side behaviour in the business-to-consumer sector as well as many aspects relevant to business-to-business contexts. We conceptualise this as the dark side of the IoT. The IoT has received much attention recently, but the dark side of IoT and its effects on provider relationships has been given little attention. Unfortunately, there is evidence that concerns in the data collection process are increasing, trust is diminishing and malicious intentions and practices are widespread and appear to be growing. For example, IoT firms may create unique IoT ecosystems and deliberately bind customers with complicated contracts, so that they are unable to use other operating systems, then bleed them with fees. This has been previously seen with insurance providers, online music services, health clubs and banks. IoT firms may confound customers with fine print and contractual obligations, and confuse and mislead customers into making poor purchase decisions through

complicated and detailed rules and conditions of the use/sale. Such practices may include confusing usage rates, penalties when customers fall short of minimum purchases or balances in their finance accounts and high penalties when customers exceed credit limits, overdrafts and payment deadlines.

Frow et al. (2011) observed that certain industries and companies infuriate customers more than others, for instance, banks, video stores, mobile phone service providers, book-purchasing clubs, health clubs, car rental companies and credit card companies seem particularly prone to dark side behaviour. Their increasing antagonistic strategies have consequently resulted in greater customer anguish and retaliation, which in turn, create dysfunctional vicious cycles. At the same time, we see that the IoT may exacerbate such vicious cycles, posing risks that are often underappreciated and as a consequence understudied. These risks include cybercrime and fraud and encompass examples such as privacy infringement, hacking, espionage and market manipulation through Internet forums and various connected social networks. These risks are external to an organisation, but often stem from internal failures in governance and control and can arise through mistakes, disgruntled employees and/or lack of integrity. It is easy to understand that the consequences for firms can be disastrous, including damaged brand reputation, reduced financial performance and corporate innovation performance (Yu, Nguyen and Chen, 2015). As the push towards IoT, smart devices and 'big data' makes clear, these risks become more and more pronounced over time, when an increasing amount of information is gathered about firms and their stakeholders. Further, the growing use of the IoT to facilitate marketing activities reveals the importance of understanding the growing challenges and risks for firms and their stakeholders, and the managerial and policy implications for curtailing such risks.

The aim of this paper is to explore the dark side of IoT from the firm perspective by looking at the abuse of relationships created through poor IoT management. We identify two

key reasons, which may result in dark side behaviour. First, a lack of a strategic focus of the IoT and lack of understanding of the integrity challenge may lead to maliciously motivated firms that can explicitly exploit customers. Second, at the tactical level, when firms use intrusive technology, poor application of IoT systems may result in inappropriate abuse of customers, as IoT technology can equip them with powerful resources to do this.

We structure our paper as follows. First, we briefly describe the nature of IoT management and the associated terms of Internet of Everything (IoE). Second, we consider the dark side of the IoT from the firm perspective and identify the different forms it can take. Third, we discuss how the negative outcomes of IoT management can be addressed through a more holistic and strategic approach involving a focus on five key strategic processes. Considering these strategic IoT processes should create awareness towards the dark side issues and their potential solutions. Finally, we identify key areas for future research.

Exploring the underlying reasons for IoT dark sides

Despite the attention given to the rapidly growing area of the IoT, there is now some evidence that IoT initiatives often become ineffective. Reports suggest there are insecure systems in the IoT industry, which is finally recognising that their track record for security issues has been poor. For example, a high profile case involving the US Federal Trade Commission's (FTC) settlement with TRENDnet (FTC, 2013) revealed that their Home CCTV system allowed strangers to see and listen into over 700 home security camera feeds because of poor security and encryption practices (Lahav, 2015; Nguyen and De Cremer, 2016). IoT critics have been reflecting on the idea whether an IoT enabled world would create a dystopian nightmare where everyone and everything will be constantly monitored and tracked. From cameras to industrial controls to GPS systems, the increased connectivity of devices leads to increased data and accordingly to security threats. This imminent danger

to the integrity of the IoT can be illustrated with Dr. Arnim Zola's algorithm in the movie Captain America 2. In the movie, Dr. Arnim Zola developed an algorithm that focused on identifying potential threats to the mother organisation, Hydra, based on personal data, such as SAT scores, social media, voting patterns and much more, to determine if specific behaviour or skills could threaten the organisation (Nguyen and Simkin, 2015).

In a similar way, it is clear that when the IoT connects all the dots, combining personal details and behaviour with excessive monitoring, it also causes or leads an integrity risk to what will happen with all that personal data, especially if it is not carefully and securely implemented. Unfortunately, the algorithm metaphor of Dr. Zola holds real merits since it is increasingly becoming the norm among knowledge driven companies to collect enormous amounts of data to predict the behaviour of their customers. What they cook, how much they exercise, in which room in the house they spend the most time and which way they drive to work, and so on, are all being recorded on the IoT via for instance, via users' different apps. The pervasive belief is that the IoT will enhance customers' lives and make them 'smarter' (intelligent), while at the same time feed data to develop the firms' competitive behaviour, making it possible to more directly, for example, target, monitor and deliver more specific and customised experiences. Yet, at the same time, talented or powerful individuals, such as CEOs and celebrities may be targeted purposefully. Clearly many IoT projects are still not implemented successfully to deliver their intended results.

Several reasons underlie the dark sides of the IoT. We consider that the IoT failure cannot be attributed to solely one factor but suggest a variety of reasons why IoT initiatives have revealed poor results. Specifically, in our search for reasons leading to the failure of IoT implementation, we focus on issues at the *tactical level*, including quality of data, project management skills, and technological skills. At the *strategic level*, we consider strategic aspects of IoT implementation, such as IoT capability and IoT networks. Further, we argue

that the lack of a clear definition of IoT has impacted the implementation of IoT negatively and its broader cousin the Internet of Everything (IoE). That is, a substantial amount of IoT let-downs can be attributed to a lack of clarity as to what the IoT encompasses and a lack of a strategic framework to guide its implementation. This starts with the absence of adopting a comprehensive definition that spells out its full scope. Consequently, the result is that IoT firms can easily exploit customers, mistaking tactically orientated data collection of customers for IoT success. Another consequence that underlies the actions of these data driven firms is that maliciously motivated suppliers may abuse customers using powerful IoT technology.

In light of the reasons that manifest in dark side firm behaviour, we observe and highlight that the severe lack of strategic focus in organisations is caused by (1) research not taking a broader, strategic focus, (2) the absence of a strategic orientation of the IoT from senior management, and (3) much operationalisation of the IoT continue to reflect a tactical, as opposed to a strategic character. We wish to argue that many organisations are engaging in tactical IoT when it comes down to the management of transactions and customers, without the overarching structure of a more holistic, strategic and co-creative approach to enhancing customer relationships within the IoT's power. Thus, such transactional-oriented and short-term focused customer management activities are misunderstood as strategic IoT, which causes more failures and dark side behaviours, which can ultimately undermine the adoption of true strategic IoT.

Apart from the importance of defining IoT in relation to a strategic framework, we assert that a critical aspect of the IoT is identifying the key strategic processes between an IoT provider and its customers. With a holistic, process orientated framework of the IoT, it is necessary to provide a useful checklist for managers; one that identifies several stages of developing the IoT along with a series of supporting conditions that impact on the IoT

implementation and its value. More frameworks are needed for the IoT, *proces*-based and focused on both tactical and strategic aspects of IoT.

To provide a holistic and process based IoT conceptualisation that brings useful insights into the IoT, we draw from Payne and Frow's (2005) framework on customer relationship management (CRM), which considers a strategic, process based cross-functional conceptualisation of CRM derived from empirical research. They identify five key processes: (1) a strategy development process, (2) a value creation process; (3) a multi-channel and customer experience process; (4) an information management process; and (5) a performance assessment process. We adapt and utilise this framework, as it details the nuanced elements within these processes and thus allows for a more thorough understanding of the IoT's multifaceted nature and activities. In the discussion section of this paper, we further consider how these activities can be managed more strategically and how dark side behaviours can be addressed.

Towards a framework of the dark side of IoT

In this paper, we refer to the dark side of the IoT as the deliberate and malicious behaviours of IoT providers with the intentions to take advantage of their customers in unfair ways. Such behaviour may result from malicious intent but can sometimes also occur through poor understanding of the IoT, all of which can lead to actions that abuse and exploit customers knowingly. Our focus is on the organisation's dark side behaviour, highlighting the provider's manipulation of the IoT for its own benefit and against the interests of other parties. Figure 1 identifies the main forms of dark side behaviour, in which we seek to classify principal manifestations of dark side behaviours. The eight types of behaviour are grouped in four broader categories based on the means used to produce dark side behaviour and the target of the dark side behaviour. We explain each of them below.

Figure 1 here.

Knowledge and intelligence-based dark side behaviour

Information and market intelligence create a smart and intelligent environment, which is an essential component to a functional IoT system and network. However, when IoT firms distort, hinder or otherwise manipulate information flows, various forms of dark side behaviour may occur. The first dark side dimension involves firms that act to manipulate knowledge for their own interests and against those of the consumer or other interested parties, as explained next.

Information misuse

As the IoT involves tracking, monitoring and assembling detailed information about customers in order to serve them better, there is a potential for the misuse of information, where vital information is used in ways that customers disapprove of. IoT firms that are able to collect and integrate information from a variety of sources may sell these to third party companies and other firms to use without the customer's knowledge or permission. Such information may include behavioural tracking, such as monitoring of usage, purchases, web and in-store tracking and similar information. Supplemented with additional information purchased from data brokers, IoT firms possess unique knowledge about their customers' behaviours, which provides the basis for carefully targeted and customised promotional campaigns based on detailed knowledge. Such powerful knowledge gives IoT firms an overhand position, weakening the position of the consumer.

Privacy issues

Firms can access information about customers from many sources via the IoT, but not all of these customers may be aware of this practice. For example, by probing into transaction records and observations of the customer's usage behaviour, firms can access detailed and readily available information that gives them more knowledge about customers' wishes. Also, sensitive information about age, employment, weight, financial statements, etc., may be available via personal gadgets, such as wearable exercise units (FitBit, Nike fuelband, smartphones apps, etc.). IoT systems may be used to keep records of customers' expenditure and may even monitor their smart refrigerators and smart waste bins for clues as to what are the customers' likes and dislikes. While this is monitored in the name of better serving customer in the future, information about usage behaviour may exceed the kind of information that some customers feel comfortable with, although the provider knows about this. Other sensitive information could include personal details, such as pornographic movie channels watched (Frow et al., 2011). The central issue is that in their pursuit of implementing a perfect IoT system, firms may desire to learn more about their customers than is desired by the customer. Annoying or invasive advertising are also examples of dark side behaviour belonging to this category. For example, spamming is an unwanted intrusion, and the Internet has led to many different forms of communication and intrusion, including pop-up ads and unsolicited e-mails offering various unwanted services. With the IoT, new forms of spamming will surge. These will become annoying, especially if they are not targeting only the intended audience.

Transaction based dark side behaviour

The second type of IoT dark side concerns situations where firms strive to profit as much as possible without considering a relationship- and long-term approach. Such practice may involve deliberately providing inferior products and services to some customers or constrain

or misdirect their choices. These examples of a short-term approach also involves offering the customer products and services with "hidden" and unexpected costs and conditions, restricting the alternatives available, or ignoring the needs of some customers, so that these IoT firms can maximise their profits from each transaction.

Confusing customers

When presented with a new IoT subscription plan, it is easy for firms to confuse or mislead customers so that the customers make decisions that are disadvantageous to them. With a complex and sophisticated technology like the IoT, confusing information is common and with firms hiding relevant information from customers, customers will be greatly disadvantaged and have difficulty in making reasonably well-informed decisions. Examples include complex pricing alternatives of IoT subscriptions, or complicated usage rates of the IoT that make comparisons of price and fees among IoT service providers very difficult. Vulnerable groups such as the young, the elderly, the poor and technologically unsavvy are particularly susceptible to this type of dark side behaviour (Frow et al., 2011). Putting pressures on consumers to make well-informed decisions is increasingly common in today's marketplace with abundant choices. The IoT comes with ever greater choice with endless customisation possibilities and differentiation, making it easy to confuse the customer, with for instance, frequent price and rate changes, such that the customer does not have enough time to adapt to the new tariffs.

Financial penalties

Deliberately profiting from financial penalties is another example of dark sides by IoT firms. Often such penalties are buried in the "small print" because service providers can make significant revenue from them (McGovern and Moon, 2007). The insurance industry has been

home to such dark side financial practices. For example, certain insurance companies request their policyholders to wear traceable devices in order to monitor their daily exercise and movement levels, which directly feeds into their health insurance policies. If the devices are not used, some penalties are imposed. Frow et al. (2011) note a situation when customers not making a payment on time are charged a disproportionate penalty. These deliberate financial exploitation of customers and the use of unfair financial penalties as a source of revenue can easily be adapted to the IoT context. As an example, penalties may be imposed for disconnecting certain IoT units or perhaps, when customers with an 'adaptable pricing plan' miss a payment, this may result in financial consequences.

Relationship-based dark side behaviour and negligence

The third dimension of IoT dark side considers dark side behaviours relating to the customer-firm relationship. As the IoT is a network in itself, this dimension may be more prevalent that others. For example, a breakdown of the IoT may occur in situations where the firm discriminates the needs of some customers and ignoring others, because they consider their profit margins to be more important than their relationships. Or when the firm makes promises of mutual beneficial outcomes (reciprocity of information provided versus benefits received), but thereafter neglects their promises. Researchers note that seemingly good relationships can go bad and close relationships that seem stable, can be vulnerable to decline and destruction (Anderson and Yap, 2005; Frow et al., 2011). When these relationships lose their ability to add further value, trust may disappear and acts of opportunistic behaviour may come to light or the relationship may simply go stale (Moorman et al., 1992). Some relationships turn bad when the asymmetry and dependence in those relationships become too overpowering. That is, when customers cannot leave (get locked in an ecosystem) or are too dependent on the supplier (perhaps receiving lesser quality of service), the consequence is a

breakdown of the IoT network, as services become ‘all things disconnected’.

Customer favouritism and discrimination

With the IoT in place, impeccable knowledge on customers exists, resulting in micro segmentation and customisation schemes based on their buying behaviour characteristics and their economic attractiveness. Two customers comparing their IoT will find very different offerings and the one considered as a high priority customer will be offered additional and superior services, while the lower priority one will not. As a result, customers who have not been prioritised are disadvantaged and will feel discriminated when they observe the superior ways other customers are treated with. Such superior services include priority services or dealing with more dedicated and better qualified personnel (Frow et al., 2011). This can have adverse effects on the IoT network. Preferential treatment is a precursor to unfairness perceptions, both towards the disadvantaged customers, but especially when the most profitable customers are treated against their expected entitlements (Xia et al., 2004).

Switching barriers and sunk costs

IoT providers can make it difficult and costly for customers to change service providers in order to retain customers. Gummesson (1994) points to the ‘hooking’ of customers into captive relationships and punishing their escape with high switching costs. Frow et al. (2011) do not consider switching costs and sunk costs as dark sides, because they arise naturally in a relationship as the parties get to know each other and invest in the relationship. They note that a dark side manifestation of switching costs exists as customer ‘lock-in’ and ‘price gouging’, referring to when a consumer commits to a service from a particular provider and is forced to buy upgrades, repair services and replacement parts from the same provider at much higher prices than they might otherwise pay. Given the significant involvement in the

IoT, we consider that switching barriers can be a dark side, especially in a situation when a provider pushes for the connection of more and more units, making the switch unreasonable. IoT predictive models can help identify where firms can profit from such behaviour, giving the firm an unfair technological advantage and thus becomes a dark side.

Integrity challenge and manipulative dark side behaviour

The last forms of dark side instances concern the lack of integrity and the negative impacts of the IoT providers' dark side behaviour on third parties when immoral conduct and manipulation is involved. These dimensions, which typically are at the personal level, consider service providers' deliberate attempts at manipulating market conditions in order to take advantage of the situation, while disadvantaging the other party.

Dishonesty

While some of the above categories may be described as dishonest, there are other dark side categories that fall more directly under the dishonesty heading. At the firm level, an IoT organisation may put pressure on their staff to up-sell and cross-sell, resulting in customers being sold products they do not need, leading to the connection of more units than warranted. Such firms typically have reward and performance systems to the detriment of their customer's interests. With the IoT in place, there may be a need for ongoing servicing to ensure that everything runs smoothly. In such cases, there may be instances of fraudulent activity, with, for example, service firms charging for replacement parts and repairs not needed and services that charge for 'blanket' screening when it is not called for. Cheating, fraud and similar behaviour, including selling products or services with known defects (Frow et al., 2011), are all examples of dark side behaviour under this category.

Unfairness

Exploitation, discrimination and the manipulation to encourage undesirable behaviour of certain groups are the results caused by a lack of integrity and a desire to treat customers unfairly. Unfairness can be defined as behaviours that are unacceptable and unjust, with particular focus on norms and values in the market place. An example includes charging Mac users higher prices for connecting to the IoT[1], or adjusting prices towards certain vulnerable groups but not to others. In 1999, Coca-Cola developed a smart vending machine that would raise the price when the weather was hot (Xia, 2015). Such smart machines will be the norm as the IoT takes foothold. In 2000, an Amazon.com customer found that a DVD, which he bought for US$26.24, dropped in price when he deleted the cookies on his computer, suggesting that the company had tracked his behaviour and raised the price due to his interest in that product (Xia et al., 2004). While these pricing practices are not illegal, many customers will feel unfairly treated, resulting in outrage, complaints and negative publicity for the company. Unfair situations and the afore-mentioned integrity challenges clearly lead to a situation of distrust, which in turn will be detrimental to the implementation of the IoT.

Discussing the integrity challenge and the implications of a holistic IoT approach

The framework presented in this paper considers the neglected area of IoT dark side practices. With the power that comes with the IoT in terms of data-driven knowledge, the increased potential for exploitation of ever-more-powerless customers is clearly present. We identify that the dark side of the IoT occurs both when firms mistake the IoT with excessive data collection, leading to customer exploitation, but also when firms are maliciously motivated to take advantage of the customers for profit. With the use of IoT technology,

[1] A similar case happened when *The Wall Street Journal* reported that Mac users were showed costlier hotel prices than Windows users by Orbitz, with as much as 30% more a night on hotels (Mattioli, 2012).

firms can take a greater slice of the value created, consequently extracting more value from customers. Such misunderstanding of a calculated IoT approach is detrimental to achieving the strategic goals of the IoT. The manifestations resulting from the dark side practices as discussed in our paper thus represent an area that should be of great concern to IoT providers, policy makers, consumers and researchers.

These dark side behaviours exist because the IoT is not viewed strategically and not enough time, energy and resources are spent on understanding the nature of the integrity challenge. As shown above, a poorly practiced IoT exists in both transactions as well as in relationship-based approaches. This is where the concept of fairness is important, in that it considers what is acceptable and just based on value and norms, and creates the necessary trust to keep long-term goals in the equation.

We believe thtypes of IoT dark side behaviour can be addressed through a fairer and more holistic approach to the IoT. To ensure that trust in the data collection process and the monitoring technology used remains, it is crucial for businesses to manage the fairness of how the data are collected and by which means. Many of the above examples violate both integrity and fairness of the IoT system, and much more needs to be done to manage the IoT's fairness. On the one hand, without fairness, evidence of exploitation, manipulation, deception and distrust may surface. However, with greater fairness, over time increased trust can be developed and a more effective and long-term view of the IoT will be realised. However, high levels of profitability do little to encourage IoT providers to address dark side practices in a socially responsible and ethical manner (Frow et al., 2011). Research on the dark side of the IoT has been given little attention and there is little or no systematic evidence about the scope of its impact, thus making it easier for IoT providers to ignore the dark sides.

Avoiding dark practices

Drawing from Payne and Frow's (2005) five key strategic processes of CRM, we now consider how a holistic approach to the IoT processes can help guide organisations away from the dark side and towards a more enlightened practice of the IoT. A holistic IoT strategy can develop from addressing the ongoing cross-functional processes of: (1) strategy development; (2) value creation; (3) multi-channel integration and customer experience; (4) information management; and, (5) performance assessment.

The first process is the *strategy development process* of the IoT. At the heart of this process is the goal of matching the customers' needs with the resources and capabilities of the organisation. Most dark side issues should be addressed at this level, but most important to consider are *knowledge and intelligence-based dark side behaviours* and *the integrity challenges and manipulative dark side behaviours*. This process provides important inputs to the value creation process.

The second process is the *value creation process,* which determines the value the supplier provides and receives from the customer and how value is co-created (e.g. Prahalad, 2004). As the focus in this process is on developing a mutual rewarding relationship, this process addresses dark side practices related to *relationship based dark side behaviour and negligence*. The objective is to co-create a mutually beneficial exchange of value over the duration of the relationship.

The third process involves the *multi-channel/customer experience process,* which seeks to ensure an integration of different customer touchpoints and communication channels. The objective is to give a consistent view of the IoT provider through interactions with the customer, in the channels that the customer prefers. This process seeks to avoid dark sides related to *transaction based dark side behaviours*. The objective is to provide a consistently superior customer experience.

The fourth process, referring to the *information management process*, seeks to address

the IoT providers' collection, storage and use of customer information. Since this is of utmost importance, it must be managed at both the strategic and tactical levels. Here the potential exists for dark side behaviours related to knowledge and intelligence-based actions. A strategic approach seeks to enhance mutual value co-creation by only using the information, which has the customers' permission. This involves, at the tactical level, having a memory of previous transactions of the customer and to use this proactively during customer interactions to deliver high levels of service quality.

The final process, the *performance assessment process*, involves monitoring all relevant IoT touchpoints, to ensure all relationships are managed for mutual value creation. This includes assessing the firm's performance across a broader range of stakeholders than only customers. This process addresses all the dark side issues on both customers and other relevant stakeholders, since continuous monitoring for fairness and integrity may prevent the dark sides from emerging.

Certainly, some of these manifestations of dark side behaviour can be addressed within more than one process. Each of these cross-functional processes interacts with the other processes. Collectively, as a consequence of adoption of a strategic and holistic approach, the processes have the potential to contribute to the improved development of fairer IoT practices. The level of fairness in an IoT ecosystem can enhance the overall trust in the IoT and with fairness and trust in place, new advancements in the IoT will not be seen as a threat, but rather as an opportunity to reveal more efficiency within the IoT relationship (Nguyen and De Cremer, 2016).

Conclusion

The subject of the IoT's dark side requires more research, as researchers in particular do not appear to have examined the long-term economic and customer impact of dark side activities.

First, future research should focus on the different motivations to manage an organisation to achieve better IoT practice. For example, the poorly functioning IoT practitioner needs to develop managerial skills to improve implementing the IoT, while dark side practitioners may require changes in strategic orientation, ethical values and/or in the culture of their organisation. Second, the forms and classification scheme for dark side behaviours developed in this paper may not be exhaustive and future research may identify more systemic dark side behaviours as they continue to emerge in the future. More empirical research is needed to seek to identify other forms of dark side behaviour and to test the different relationships proposed in the framework. Third, future research should identify the scope and scale of dark sides' impact on economic, social and societal environment. Ramifications exist for many stakeholders, including government, consumers, and more generally connected third parties.

Fourth, there is a need to identify whether dark side practices are more prevalent in some industry contexts than in others and whether the impact of dark side practices varies from industry to industry (Frow et al., 2011). Fifth, other dark side concepts - such as opportunism and greed - may need to be classified, as well as other possibilities. Certain dark side activities may be driven by other underlying dark side behaviours; something that needs to be explored further. Deeper examination of dark side practices may be studied in qualitative research approaches. Finally, greater attention needs to be directed to making dark side practices more visible and more research is needed to learn how the dark sides can be addressed successfully, so that the IoT providers can avoid the resulting damages of dark side behaviours during their interactions with customers. Understanding the social and ethical consequences of dark side behaviour enables addressing some of the negative outcomes of the IoT that have been considered in this paper.

In this commentary, we are seeking to add to an ongoing debate by identifying and raising awareness of the underlying *dark sides* of the IoT. We consider the IoT's influence on marketing and the dysfunctional forms of the IoT, which are neglected as an area of research in general. By identifying the different types of IoT providers' dark side behaviors, we develop an integrated approach to the IoT that will support overcoming these dark side behaviors.

References

Anderson, E. and D.S. Yap. (2005). "The dark side of close relationships." *MIT Sloan Management Review* 46 (3): 75-82.

Frow, P.E., A. Payne, I.F. Wilkinson and L. Young. (2011). "Customer management and CRM: addressing the dark side." *Journal of Services Marketing* 25(2): 79–89. http://dx.doi.org/10.1108/08876041111119804

FTC (2013). "Marketer of internet-connected home security video cameras settles FTC charges it failed to protect consumers' privacy." *Federal Trade Commission*, Press Release, 4 September 2015, https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles [Accessed 8th October 2016]

Gartner (2015). "Gartner says 6.4 billion connected "things" will be in use in 2016, up 30 percent from 2015". Press Release, STAMFORD, Conn., November 10, 2015. http://www.gartner.com/newsroom/id/3165317 [Accessed 8th September 2016]

Gummesson, E. (1994). "Making relationship marketing operational." *International Journal of Science Industry Management* 5(5): 5-20. http://dx.doi.org/10.1108/09564239410074349

Lahav, S. (2015). "The dangers of IoT and how to mitigate the risks." *IT Pro Portal,* 2 August 2015, http://www.itproportal.com/2015/08/02/dangers-of-iot-how-to-mitigate-risks/ [Accessed 8th October 2016]

Mattioli, D. (2012). "On Orbitz, Mac users steered to pricier hotels." *The Wall Street Journal,* 23 August 2012. In Nguyen, B., Simkin, L, and Canhoto, A. (2016). *The Dark Side of CRM: Customers, Relationships and Management,* (Eds) Routledge, London, UK, (p. 39).

McGovern, G. and Y. Moon. (2007). "Companies and the customers who hate them."

Harvard Business Review, June: 78-84.

McKinsey Group. (2015). "Unlocking the potential of the Internet of Things." http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world [Accessed 8th September 2016]

Moorman, C., G. Zaltman and R. Deshpande. (1992). "Relationships between providers and users of market research: the dynamics of trust within and between organizations." *Journal of Marketing Research* 29: 314-28. http://www.jstor.org/stable/3172742

NCTA (2015). https://www.ncta.com/platform/broadband-internet/behind-the-numbers-growth-in-the-internet-of-things-2/ [Accessed 31/01/2016]

Nguyen, B. and D. De Cremer. (2016). "The fairness challenge of the Internet of Things." *European Business Review*, January/February (pp. 31-33) http://www.europeanbusinessreview.com/?p=8588 [Accessed 8th October 2016]

Nguyen, B. and L. Simkin. (2015). "The dark side of the Internet of Things." *Journal of Marketing Management Blog*, 20th November 2015 http://www.jmmnews.com/the-dark-side-of-the-internet-of-things/ [Accessed 8th October 2016]

Payne, A. and P. Frow. (2005). "A strategic framework for customer relationship management." *Journal of Marketing* 69: 167-76. http://dx.doi.org/10.1509/jmkg.2005.69.4.167

Snyder, M. (2015). "The Internet Of Things: A dystopian nightmare where everyone and everything will be monitored on the Internet." http://www.washingtonsblog.com/2015/03/42846.html [Accessed 31/01/2016]

Woodside Capital Partners (2015). THE INTERNET OF THINGS "Smart" Products Demand a Smart Strategy Using M&A for a Competitive Edge. Report http://www.woodsidecap.com/wp-content/uploads/2015/03/WCP-IOT-M_and_A-REPORT-2015-3.pdf [accessed 12 September 2016]

Yu, X., B. Nguyen and Y. Chen. (2015). "Internet of Things capability and alliance: entrepreneurship orientation, market orientation, and product and process innovation." *Internet Research* 26(2): 402-34. http://dx.doi.org/10.1108/IntR-10-2014-0265

Xia, L. (2015). "Perceptions of fairness and unfairness." In Nguyen, B., Simkin, L., and Canhoto, A. (2015). *The Dark Side of CRM: Customers, Relationships and Management,* (Eds) Routledge, London, UK, (p. 39).

Xia, L., K.B. Monroe and J.L. Cox. (2004). "The price is unfair! A conceptual framework of price fairness perceptions." *Journal of Marketing* 68(4): 1–15. http://dx.doi.org/10.1509/jmkg.68.4.1.42733

Figure 1 A Framework of the Dark Side of the IoT