Social media? It's serious! Understanding the dark side of social media

Christian V. Baccarella [a, *], Timm F. Wagner [b], Jan H. Kietzmann [c], Ian P. McCarthy [d]

[a] Friedrich-Alexander-Universität Erlangen-Nürnberg, Lange Gasse 20, 90403, Nürnberg, Germany
[b] adidas AG, Adi-Dassler-Strasse 1, 91074, Herzogenaurach, Germany
[c] Gustavson School of Business, University of Victoria, 3800 Finnerty Rd, Victoria, BC, V8P 5C2, Canada
[d] Beedie School of Business, Simon Fraser University, 500 Granville Street, Vancouver, BC, V6C 1W6, Canada

ARTICLE INFO

Article history:

Keywords:
Social media
Dark side
Unintended consequences
Bullying
Fake news
Trolling

ABSTRACT

Research and practice have mostly focused on the "bright side" of social media, aiming to understand and help in leveraging the manifold opportunities afforded by this technology. However, it is increasingly observable that social media present enormous risks for individuals, communities, firms, and even for society as a whole. Examples for this "dark side" of social media include cyberbullying, addictive use, trolling, online witch hunts, fake news, and privacy abuse. In this article, we aim to illustrate the multidimensionality of the dark side of social media and describe the related various undesirable outcomes. To do this, we adapt the established social media honeycomb framework to explain the dark side implications of each of the seven functional building blocks: conversations, sharing, presence, relationships, reputation, groups, and identity. On the basis of these reflections, we present a number of avenues for future research, so as to facilitate a better understanding and use of social media.

© 2018 Published by Elsevier Ltd.

1. Introduction

Over the past decade, social media have been transforming how individuals, communities, and organizations create, share, and consume information from each other and from firms. What appeals to almost 90% of the younger EU citizens (Eurostat, 2017a) is how social media differ from traditional media (e.g., newspaper and television) in terms of their reach, interactivity, usability, and ubiquity. In 2017, users spent more than 2 hours on average per day on social networks and messaging services (half an hour each day longer than five years earlier), which amounted to about one third of their entire daily computer time (Mander, 2017).

Many studies have touted the advantages that social media would bring to individuals and firms (e.g., Kumar, Bezawada, Rishika, Janakiraman, & Kannan, 2016; Sabate, Berbegal-Mirabent, Cañabate, & Lebherz, 2014; Wagner, 2017). They highlight the "bright side of social media" and how engagement between firms and consumers is being democratized (Kietzmann, Hermkens, McCarthy, & Silvestre, 2011). For firms, this means social media would improve marketing, public relations, customer service, product development, personnel decision-making, and other business activities that rely on information exchanges and engagement with consumers and employees. Many of these advantages have materialized, thus leading almost 50% of all EU firms to use at least one form of social media in 2017 (Eurostat, 2017b). These firms use social media to not only broadcast company content but also track sentiment worldwide by analyzing user-generated content (Paniagua, Korzynski, & Mas-Tur, 2017), consumer-generated intellectual property (Berthon, Pitt, Kietzmann, & McCarthy, 2015), and interactions on social networking sites (Wagner, Baccarella, & Voigt, 2017), to adjust their business and marketing strategies appropriately.

Regardless of the numerous opportunities social media offer, an increasing number of incidents demonstrate that there is undoubtedly a "dark side" to social media. Chamath Palihapitiya, a former Facebook executive, recently stated that he regrets that some of the tools he has helped to create "are ripping apart the social fabric of how society works" (Wong, 2017). This quote vividly illustrates how the qualities that underlie the enormous presence of social media platforms are now also undermining the freedoms and the well-being of the individuals and communities they serve. For example, there have been an increasing number of reports and research attention into concerns such as cyberbullying (O'Keeffe & Clarke-Pearson, 2011), trolling (Buckels, Trapnell, & Paulhus, 2014; Hardaker, 2010), privacy invasions (Pai & Arnott, 2013), fake news (Allcott & Gentzkow, 2017; European Commission, 2018), online

firestorms (Pfeffer, Zorbach, & Carley, 2014), and addictive use (Blackwell, Leaman, Tramposch, Osborne, & Liss, 2017). Furthermore, a 2017 survey found that Britons aged 14—24 believe that social media, such as Facebook, Instagram, Snapchat, and Twitter, exacerbated self-consciousness and "fear of missing out" (Przybylski, Murayama, Dehaan, & Gladwell, 2013), which can result in increased levels of anxiety, sleep loss, and depression (e.g., Levenson, Shensa, Sidani, Colditz, & Primack, 2016). In the workplace, a recent study found that the benefits of social media also come with negative consequences through work-life conflicts and interruptions that increase exhaustion (van Zoonen, Verhoeven, & Vliegenthart, 2017).

Even with social media executives admitting that their platforms have deleterious impacts, users tend not to question the short- and long-term implications and potential risks of their choices. Many company employees and customers now belong to a generation of digital natives who have grown up with social media, rather than first learning to use these technologies as adults (Bennett, Maton, & Kervin, 2008). Most adult users, too, have become so accustomed to social media that the types of conversations, self-expression, community building, and other forms of online engagement are now parts of the only reality they know. It is therefore of utmost importance to take a step back to reflect on how we have arrived at the present and what our most recent social media "advances" might mean for us in the future.

In this article, we draw attention to the duality of social media: for the many bright sides of social media, there are also dark sides that are worthy of being investigated so that we become more conscious of their potential risks and make better-informed decisions. We begin by clarifying what we mean by the dark side of social media, and why it is a concern for society. We then introduce a framework for understanding the dark side of the core functionalities of different social media platforms. By using the ideas and issues that this framework highlights, we then outline a number of important research opportunities that could help in facilitating a healthier use of the "media" by better understanding their related negative impact on the "social" fabric of society.

2. The darkness of social media

With the expression "dark side," we highlight that social media like many phenomena, including fast food (Schlosser, 2002), entrepreneurship (Beaver & Jennings, 2005), capital markets (Scharfstein & Stein, 2000), crowdsourcing (Kietzmann, 2017; Wilson, Robson, & Botha, 2017), and the sharing economy (Malhotra & van Alstyne, 2014), can have negative or detrimental consequences on society that are worthy of research attention. However, it is important to recognize that social media are not good *or* bad, helpful *or* unhelpful, black *or* white, and bright *or* dark. The consequences of many technological innovations, intentional and unintentional, are usually not dichotomous, but simultaneously have both bright *and* dark sides. When Alfred Nobel invented dynamite in 1866, he called it "Nobel's Blasting Powder." It significantly improved mining, quarrying, and construction, but of course, it also "improved" warfare when armies realized the weaponized potential of dynamite explosions. In a similar duality, we use social media to connect to our far-away friends, *and* at the same time, we disconnect from those who sit across the table from us. Importantly, these new types of engagement have long-term implications. The "shallowing hypothesis," for instance, suggests that certain types of social media activity (e.g., sharing and conversing) lead to a decline in ordinary daily reflective thinking and instead promote quick and superficial thoughts that can result in cognitive and moral triviality.

With social media, the degree of brightness or darkness is often

a subjective matter. When Rachel Burns in the UK posted a photo on Facebook of her singalong activity with residents at the care home at which she worked, she joined the many others who have been fired for a sharing faux-pas (Karl, Peluchette, & Schlaegel, 2010; Schmidt & O'Connor, 2015). While she, the people in the photo, and likely much of the UK public thought the posting was well intentioned and harmless, her employers saw it as a breach of privacy rules. In the end, the Facebook posting cost Burns her job, after 21 years of service. In contrast, few would argue with the intense darkness of the case of Britain's Richard Huckle, who created an online leader board and awarded himself and others "pedopoints" for sharing original and new recordings of sexual crimes against minors on social media (Wolak, Liberatore, & Levine, 2014). The degree to which perpetrators are aware of the nature of their actions varies, too. Cyberbullying may be a way to intentionally harm individuals, while oversharing photos of positive experiences unintentionally causes anxiety among those who live lives less glamorous. Moreover, some actions require technological savvy (e.g., gamification of criminal behavior and hacking), whereas others rely on the use of blunt tools (e.g., posting videos online).

As the attraction, use, and impacts of the bright side of social media can be studied and understood using a multidimensional honeycomb framework based on seven social media building blocks (Kietzmann et al., 2011), the impacts of these dimensions on society can also be dark, separated by various shades of gray. Thus, to understand how social media can also lead to undesirable outcomes for individuals and communities, we now employ this framework in the next section of this paper.

3. The dark side of the seven building blocks of social media

To understand how individuals, communities, and organizations can use different social media platforms to connect, monitor, and engage with each other, Kietzmann et al. (2011) developed a honeycomb framework. This framework unpacks social media functionalities into seven building blocks (see Fig. 1) to describe different features of the social media user experience and the extent to which different social media are driven by each functionality. These functionalities refer to the extent to which users can (i) converse with each other, (ii) share content, (iii) let others
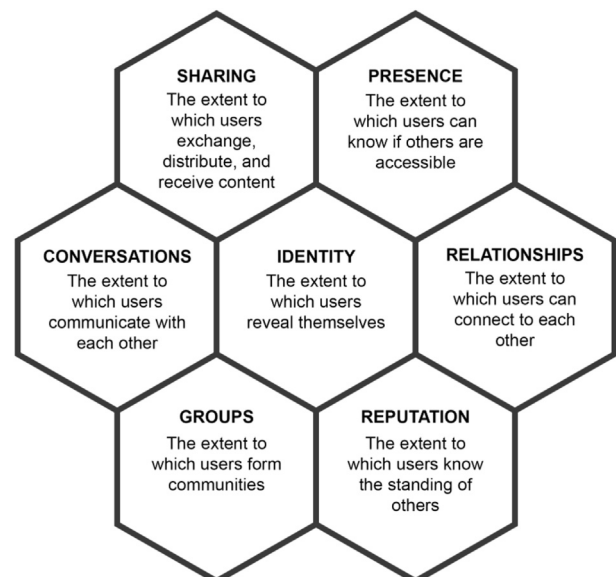

Fig. 1. Social media functionality (Kietzmann et al., 2011).

know about their presence, (iv) form relationships, (v) know the reputation of others, (vi) form groups, and (vii) ultimately reveal their identity (Kietzmann et al., 2011). A large number of studies show how different social media platforms use these functions of the honeycomb framework to different degrees to achieve specific business functions or the aims of an overall business model for the organization (e.g., Moorhead et al., 2013; Smith, Fischer, & Yongjian, 2012; Zhou & Wang, 2014).

Given the honeycomb framework's usefulness in understanding the functional building blocks of social media, we suggest that each functional block of the framework can also be used to help to understand and examine different aspects of the dark side of social media. Focusing on the negative consequences that consumers and communities face from social media, we now explain the dark side implications of each functional block (see Fig. 2). The explanations are not exhaustive but based on prototypical behaviors and examples.

3.1. Conversations

This building block refers to the extent to which users communicate with others using a social media platform. Twitter, Facebook, Instagram, LinkedIn, and many other platforms provide the ability to converse with functions such as "Like," "Reply," "Comment," and "Direct Message." For more detailed conversations, blogs provide a forum for users to post and discuss diary-style commentaries, which readers can then comment on or even add to. Further, Reddit, which at the time of writing this article was ranked the 6th most visited website in the world (Alexa Internet, 2018), is essentially a bulletin board system for over 200 million unique users who each month discuss and vote on content covering a vast array of topics, such as news, entertainment, sport, health, music, and literature.

The dark side of the conversation functionality is that excessive, aggressive, and inaccurate engagement can occur. For example, despite having clear rules and significant moderating resources intended to prohibit harassment, Reddit users can be exposed to threats and bullying. In 2010, a Reddit user who had genuinely donated a kidney made a posting seeking donations to a related charity. Some Reddit users thought this was a scam and contacted

the user at his home with death threats. Further, in 2013, Reddit admitted that its platform had helped to fuel "online witch hunts" when groups of users had wrongly named several people as suspects in the Boston bombing (BBC News, 2013; Suran & Kilgo, 2017). Furthermore, with the advent of artificial intelligence-powered chatbots and social bots that mimic human behavior and conversations, social media platforms often surreptitiously use these bots to pollute conversations in online spaces with spams and misleading advertisements (Ferrara, Varol, Davis, Menczer, & Flammini, 2016). The contributing editor of *Scientific American Mind* and former editor in chief of *Psychology Today*, for instance, was fooled into thinking a chatbot on a dating service was interested in him romantically (Epstein, 2007). But even the tools can be victims that in turn can contribute to dark conversations. When Microsoft released its Tay chatbot in 2016 to engage with millennials through Twitter, for example, some users tricked the chatbot into learning how to make racist statements (Wolf, Miller, & Grodzinsky, 2017).

3.2. Sharing

This aspect of a social media platform concerns the extent to which consumers exchange, distribute, and receive content. Consider for example how people use Flickr to share photos, YouTube to share videos, and Instagram to share photos and videos. Along with the content produced by the conversation functionality of social media, the content shared by social media users often constitutes user-generated content (UGC), i.e., the audio, video, images, and text created by users of an online system (Berthon et al., 2015; van Dijck, 2009). Successful social media platforms understand how to build on the user motivations for sharing different content along with the relationships and groups that can be produced from these motivations (Kietzmann et al., 2011).

Once users can easily share content, a fundamental risk is that the shared content can be inappropriate and undesirable or that it can be shared without permission from the holder of any intellectual property rights (IPR) associated with the content. In terms of inappropriate content, a survey of 10,000 European children aged 9–16 reported that 40% of children expressed shock and disgust when viewing violent or pornographic content that had been shared by others online (Livingstone, Kirwil, Ponte, & Staksrud, 2014). Conversely, investigations by news agencies revealed that more than 100 websites that posted fake news about the 2016 U.S. presidential election were run by teenagers in the small town of Veles, Macedonia (Allcott & Gentzkow, 2017). For IPR infringement risks, consider for example the case of Stephanie Lenz who, in February 2007, posted a 29-second video on YouTube of her baby pushing a toy around the kitchen, while dancing to the song "Let's Go Crazy" by Prince that was being played in the kitchen. In June 2007, the Universal Music Group (Universal), which manages the copyright of Prince's music, decided that the song rather than the dancing baby was the focal content in the video. Universal issued a takedown notice to YouTube, and the video was immediately removed from the website. Lenz disputed the removal of the video and filed a "counter-notice" to YouTube, arguing that no rights of Universal were violated by her video. Universal insisted that sharing the video was wilful copyright infringement and that Lenz was liable to a fine of up to US$150,000 (Lessig, 2008). In sum, it is clear that the powerful and addictive sharing functionality of social media presents risks to those who share content and those who consume the content that is shared.

3.3. Presence

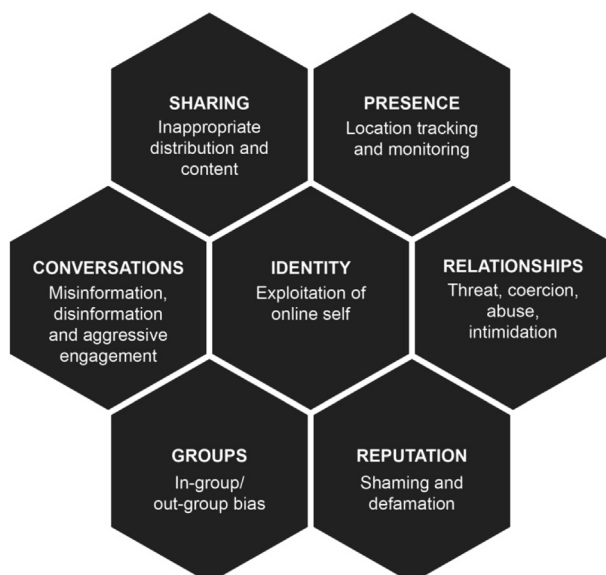This functional block concerns the extent to which

Fig. 2. The dark side of social media functionality.

organizations and individuals know whether, where and when, others are accessible. This includes knowing the presence of others in an online world and/or in the real world. For example, Facebook, Trapster, Google Maps, and other social media use internet protocol (IP) address information, location information from mobile devices, and "check-in" declarations to monitor where individuals are and possibly allow others to know this information too. This status about one's presence allows others to communicate synchronously (Elaluf-Calderwood, Kietzmann, & Saccol, 2005) and to have higher levels of intimacy and immediacy (Kaplan & Haenlein, 2010), which results in more influential interactions.

The dark side of this functionality is that the location and availability of users are known and can be tracked without their awareness or consent. For example, in 2011, Facebook launched the Messenger application for mobile devices. From 2011 to 2015, the default settings for this application were to collect and display geolocation information with message content in the conversations. In 2012, a number of organizations reported privacy concerns about the implication of this geolocation sharing feature of the application (Cipriani, 2012), but to no avail. The policy was not changed. Then, in 2015, an extension for the Chrome browser named Marauders Map (after the magical map in the Harry Potter books that reveals by magic the location of each person) was developed and made available by a Harvard University computer science and mathematics student (Nosouhi, Qu, Yu, Xiang, & Manuel, 2017). This extension used Messenger data to map, and thus stalk, the identity, locations, and movements of all individuals in a conversation. In the dark side context, the presence building block is very directly tied to issues pertaining to protecting or invading the privacy and possibly the safety of people who engage on social media.

3.4. Relationships

This building block is concerned with the extent to which users can relate to other users through social media platforms. In other words, users have some form of an association that determines why they engage with each other and the what-and-how of the content they exchange. For example, LinkedIn's 500 million users are largely structured around professional relationships based on who users work for, work with, and where they work. In contrast, Facebook is based on friendships of all kinds, including those based on residential address, educational institutions attended, and associations with "friends of friends."

When social media help to establish and reveal relationships, they enable different types of social engagement and related deleterious consequences. This includes cyberbullying, stalking, and online harassment (Kwan & Skoric, 2013), where estimates are that 10–40% of the youth are victims of cyberbullying (Kowalski, Giumetti, Schroeder, & Lattanner, 2014), and 40% of those who cyberbully report they do so for fun (Raskauskas & Stoltz, 2007), possibly connected with occurrences of jealousy. This is because heavy users of social media are more likely to believe that others have better and happier lives (Chou & Edge, 2012), and those who live vicariously through others online have significant maintenance demands and access social media platforms excessively for the fear of missing out (Fox & Moreland, 2015).

3.5. Reputation

Reputation is the degree to which users can identify and influence the standing of others, including themselves, in a social media setting. It is a construct that can be viewed in terms of how individuals display competence (functional reputation), demonstrate social norms (social reputation), or appear to be attractive,

fascinating, or inspiring (expressive reputation) (Eisenegger, 2009). The reputation of a social media user can be indicated by, for example, the number of followers someone has on Twitter, the sentiments of the comments expressed about a social media user, the view and like counts for a user's YouTube video, or the status some platforms award to users (e.g., the influencer status on LinkedIn).

A major reputation risk stems from sharing inappropriate content, which can destroy the sharer's reputation and/or the reputations of others. Regardless of whether a posting is based on true or false content, the more outrageous the posting, the quicker it tends to spread and harm reputations. Every year, numerous business and political leaders, and others, are forced to resign after posting offensive, disingenuous, or ridiculous content on social media. To protect employers' own reputation, during hiring, they often review applicants' profiles on social media to see whether they have posted inappropriate content (Roulin, 2014); and 44% of adults in 2010 searched for information about someone who they sought to engage in a professional capacity (Madden & Smith, 2010). Certainly, there are numerous reasons not only for celebrities but also for everyday citizens to pay attention to their online standing and to be on high alert. Blogs such as Gawker and Wonkette have helped to destroy the reputations of many public figures, whereas Hollaback!, Don't Date Him Girl, and "revenge porn" sites provide platforms for users to shame, hurt, or reprimand others (Woodruff, 2014). Despite the long-term consequences of their actions, in an online setting, users revealed that they did not properly think about their reason for posting, misjudged who could be the audience, were highly emotional when posting, or were under the influence of drugs or alcohol (Wang et al., 2011).

3.6. Groups

This building block ascribes the function that social media users can create or join circles of friends or communities centered around a shared practice or interest. On Facebook, people participate in these open or closed groups (or those hidden to non-members) for socializing, entertainment, self-status seeking, and information purposes (Park, Kee, & Valenzuela, 2009). Associated benefits for the users are the possibility to organize their growing social network and to allow permissions what content can be accessed by specific (sub-)groups, e.g., what photos will be displayed on a contact's timeline on Facebook. Next to the managing function of this aspect, being part of a specific group on social media may also act as a signal to make other users aware with what kind of interests or values one can identify with.

The negative side of the groups building block, for instance, often shows its face through what social psychologists refer to as "ingroup-outgroup bias" (Tajfel & Turner, 2004). People define themselves in terms of social groupings (ingroup identity). They find themselves in an echo-chamber in which their own beliefs are amplified and reinforced, and those who do not fit into those groups (outgroups) are belittled. The "ingroup love and outgroup hate" (Brewer, 1999) can be seen when people not only exclude others from conversations or group membership but also lose empathy for them (i.e., the intergroup empathy gap). The many polarized discussions of racial and gender (in)equality serve as appropriate examples, as do the recent populist elections, and more generally, the separation of leaders and influencers vs. the general public online (Hogg & Reid, 2006).

3.7. Identity

Presenting one's identity is a central aspect of social media. Next to providing objective personal information, such as gender or age,

users can also provide more subjective details that express their identity by, for example, joining groups with a specific topic or by liking, disliking, or commenting on content. Setting up a profile and therefore becoming identifiable is a prerequisite for most social media applications. Although each user can generally decide for him-/herself what kind of personal information they want to share, social media sites have a great interest that users share as much information as possible.

Displaying one's identity online, however, has many downsides. The other building blocks (e.g., the conversations and relationships online, the sharing of images, the location-specific data, the ingroup-behavior, and the online reputation) have a direct impact of who we are, to our personality and character. The visibility, transparency, permanence, and granularity with which social media content *online* connects to people's lives *offline* emphasizes that social media users are not in control of their own identity any longer, thus leading to all sorts of privacy and safety risks. A recent UK study found that the lack of privacy and protection on social media is one major concern of children and young people (The Children's Society, 2018). Some have even gone so far as to say that stalking others on social media has already become a normality. For example, returning to the Facebook or Instagram profile of former partners and spouses to see what they are up to is nowadays considered as relatively harmless (Lyndon, Bonds-Raacke, & Cratty, 2011). Using our identity against us is also an issue in the business context. Despite potential privacy issues, searching online for private profiles appears reasonable in order to gain a comprehensive picture of a job applicant (Fuchs, 2014). Such snooping behavior is strongly supported by many social media platforms. For instance, in Europe, a report commissioned by the Belgian Privacy Commission stated that the largest social media platform, Facebook, does not provide appropriate control mechanisms concerning user data. It highlights that Facebook's default privacy settings are so difficult to find and change that the automatic and common outcome is behavioral profiling by the platform (van Alsenoy et al., 2015).

Utilized individually and together, these seven building blocks can help researchers and managers make sense of the multidimensionality of various dark side phenomena we observe today. In Fig. 3, we illustrate how two common harmful social media activities (trolling and fake news) occur through different degrees of dark social media functionality. The darker the color of the block, the greater is the role of this functionality in the example deleterious social media activity.

Trolling, in fishing, is a method where one moves the fishing lines slowly back and forth, dragging the bait through the water and hoping for a bite. Trolling on social media is much the same — so-called trolls bait others by posting inflammatory lines (messages in the conversations block) or sharing inappropriate content (in the sharing block) and then wait for a bite on the line. The intent is to provoke members of an online community (groups block) and to disrupt normal, on-topic discussions, relationships, or reputations. The motivation for trolling is not to stimulate thought-provoking discussions but to sow discord on the Internet and get a rise out of people simply for the amusement of the troll. Trolling usually happens in online forums, YouTube comments, or on Reddit, but it can also happen in organizational contexts. Employees who send malicious messages and leave touchy comments for their co-workers bring distraction to team work, decrease motivation, and impact effectiveness. Sometimes, trolls find entertainment in wasting organizational resources by taking up the time of customer support representatives, for instance in pointless Twitter exchanges or in lengthy, off-topic LiveChat conversations.

Fake news are "pseudo news" that are presented as being factually accurate, without truly being based on actual facts. Such news are either fabricated by disseminating information on social media that is deliberately false (i.e., disinformation) or the result of accidental, honest mistakes (i.e., misinformation) (see Hannah, McCarthy, & Kietzmann, 2015). In both cases, the degree of truthfulness in the news on social media is difficult to determine, because the authenticity of the news source is almost impossible to verify (as opposed to the certainty of traditional media outlets, like the Washington Post). However, the popular appeal and often sensational nature of fake news attracts millions of readers. According to Buzzfeed's Craig Silverman, during the 2016 U.S. presidential election, the top 20 fake news stories received more engagement on Facebook than the top 20 news stories on the election from 19 major media outlets (Chang, Lefferman, & Pedersen, 2016). Whether they truly influenced the outcome of the election is a different matter, but the intention of the fake news was clearly to create a greater separation between groups (e.g., voters) by seeding disinformation into online conversations,
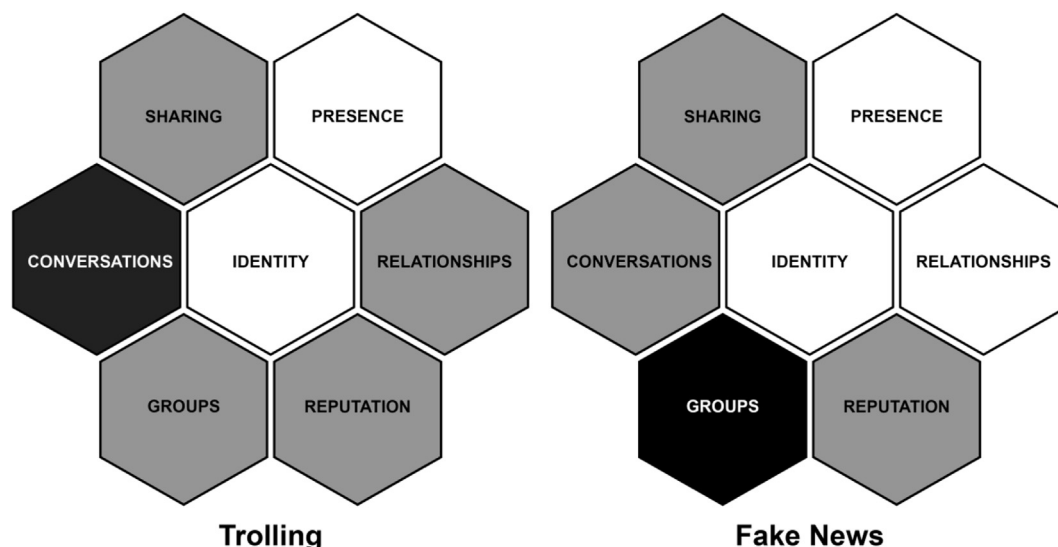

Fig. 3. Contrasting the dark functionalities of trolling and fake news.

sharing inappropriate content, and shaming and defamation of the opposite party. But fake news are not just about celebrities and politicians. Brands can be negatively affected, too. Pepsi's CEO, for instance, was said to have told Trump fans to "take their business elsewhere," a false statement that led to an online firestorm (a "sudden discharge of large quantities of messages containing negative word-of-mouth and complaint behavior against a person, company, or group in social media networks," Pfeffer et al., 2014, p. 118) and a threatened boycott of Pepsi's products. Snopes, an online fact-checking website, lists many similar fake news stories. The sportswear company New Balance, for instance, was falsely praised as the "official brand of the Trump Revolution," thus leading customers who opposed the candidate's agenda to burn their New Balance shoes (Gupta, 2016). But fake news do not only impact big brands. Fake news about any publicly traded company, small or big, can truly influence its share value, allowing those who seed the fake news to potentially realize a healthy financial gain at the expense of the firm. Or fake news can harm the reputation of a firm and place its closest competitor in a favorable position, dissuade potential employees, and harm relationships with other stakeholders.

These two examples show the descriptive, explanatory, and comparative value of using the honeycomb framework to understand the dark side and the social media landscape more generally. The framework thus provides a basis to guide the development of appropriate strategies to use and consume social media, which we now discuss in our call-to-action for researchers.

4. Don't be afraid of the dark: a call-to-action for social media researchers

To shed light on and lighten the dark side of social media, a report by the European Commission (2018) recommended to refrain from simplistic approaches but rather to respond with a "multidimensional approach" to the many social media phenomena that have reared their ugly heads. The report illustrates the inherent complexity of these issues and emphasizes the urgency to find appropriate answers to counteract further unfavorable developments. In this reflections article, our goal was to promote a similar multidimensional approach in order to understand how social media can lead to undesirable outcomes for individuals, communities, or organizations. With this goal, our "dark side honeycomb framework" suggests that combinations of identity, presence, relationships, conversations, groups, reputations, and sharing are key constructs of the dark side phenomena we observe today.

The development of the dark side honeycomb and its seven functional building blocks is one initial option toward this goal. We hope that it serves as a useful foundation for further research and motivates more researchers to take "a walk on the dark side" so as to understand the risks and how social media can help individuals, communities, and organizations engage effectively and safely online. With this goal, we pose the following three calls-to-action, each of which offers multiple avenues for future management research.

4.1. Build dark side-orientated social media theories, models, and classification frameworks!

The intention of this article was to illustrate the seven building blocks of the dark side of social media, in great part to motivate further research that tries to untangle the underlying mechanisms in new ways. Existing theories cannot necessarily be transferred to the social media sphere (Naylor, Lamberton, & West, 2012). New theories, or combinations of existing theories, might better suit the inherent characteristics of social media, akin for example, to

Scheiner, Krämer, and Baccarella (2016) who base their theoretical framework to explain unethical behavior on social media by entrepreneurs on the concept of moral disengagement and regulatory focus theory. We believe that our dark side honeycomb framework can help to motivate and guide the combination of lenses from different disciplines in order to develop novel theories, models, and classification frameworks that shed light on the dark side of social media.

4.2. Use adequate methodologies for online and dark contexts!

There is a significant opportunity for future research studies using contemporary methodologies that suit the characteristics of social media. For instance, a recent and effective development for understanding online behavior might be netnography (a portmanteau of *Internet* and *ethnography*), which allows researchers to study social interaction in modern digital communication contexts. However, a lot has happened since its introduction by Kozinets in 1998: smart phones with high-definition cameras, ubiquitous data networks, and social media networks that did not exist at all. The activities in the sharing building block of the dark side honeycomb, for instance, certainly were not the same before the widespread adoption of these tools, and neither were likely any of the other building blocks. These technological developments and their pervasiveness in our society certainly warrant the advancement of digital data collection and analysis methodologies. Especially in light of recent advancements (e.g., artificial intelligence-powered social media content analysis tools included in IBM Watson), we hope that fellow researchers will develop and test new ways in which we can study the dark side of social media.

4.3. Collect data and build cases!

Many of the dark side examples reported in this article were drawn from accounts in the popular press. The reasons for this are clear — there is a dearth of data and case studies based on rigorous data collection and appropriate analysis methodologies. Research on the dark side of social media is sparsely populated with studies that are narrowly focused or that include actual empirical data. Most are conceptual and at a rather high level, and we hope that the dark side honeycomb allows researchers to focus their work more narrowly. We call for empirical work specifically on dark side antecedents and motivations (e.g., why individuals, communities, and organizations deliberately engage in dark side behaviors and practices), on accidently or unintentional dark side outcomes, behaviors, and practices (e.g., social media faux pas), and on dark side management strategies (e.g., how individuals, communities, and organizations aim to minimize, prevent, or respond to the dark side of social media). We would further like to see more granularity in all these research streams to differentiate, when appropriate, by region, industry, and sector (e.g., Europe vs. North America, not-for-profit vs. for profit, and private vs. public) and social media phenomena (e.g., hashtag hijacks, culture jamming, reputation blackmail, online firestorms, online bullying and workplace tensions, tweet-up disasters, and activities on the darknet/dark web/deep web).

Our three calls-to-action (i.e., for more work on theory and conceptual frameworks, on advancing methodology, and on focused empirical studies) are suggestions, which we hope provide inspiration to attract researchers to the dark side.

5. Final thoughts

"Social Media is everywhere" is how Kietzmann et al. (2011) article first introduced the honeycomb framework. Seven years

later, social media have truly become ubiquitous. But unlike in 2011, the news surrounding social media are no longer just cheerful and bright. Instead, the popular press usually informs us about new instances of how social media have fueled intellectual property leaks, fake news, privacy invasions, election meddling, etc. The tone has changed, and we are becoming keenly aware of how deeply the dark side of social media impacts our private and business lives.

As private individuals, although we know better, we continue to use social media with little regard to its darker side. We continue to upload pictures and videos of our children without their consent and start a digital presence they will never be able to reclaim. We install new apps on our phone without reading the end-user-license agreement, and we give away our (and our friends') Facebook data in exchange for free Wi-Fi. We take and post pictures of our food for distant friends instead of enjoying the moment with our loved ones at the table. It has become normal for people to "slutshame" and post "revenge porn" of their former partners — two terms that did not even exist a decade ago but are common among adolescents today. Children are losing their sense of empathy, because when they insult someone online, they no longer see the impact of their actions and the sadness of their victims' faces. And like them, hiding behind online anonymity, adults are quick to judge others publicly, without really knowing all the necessary details. On social media, people are guilty until proven innocent, and then, it is usually too late for their reputation to recover. While social media offer us previously unforeseeable levels of connectedness and with it offer tremendous advantages (e.g., the collective power behind the "#metoo" movement against sexual harassment), we simultaneously see levels of online harassment, bullying, vigilantism, etc. increase sharply.

For organizations, the cost of "social media gone bad" is difficult to quantify, but the consequences can nevertheless be dire. When in 2009, musician Dave Carroll unsuccessfully attempted to recover the cost for the Taylor guitar United Airlines' baggage handlers destroyed, he composed a song about United that went viral and led to an undesirable impact for United Airlines. Millions watched the video shared on YouTube, which some attributed to the fall in stock value shortly after. Social media are nonforgiving, brands are held to increasingly high standards and are immediately punished for their missteps. What is most surprising, possibly, is that brands frequently do not appear to learn from social media fails. Every single year sees many companies, big and small, causing uproar online for their actions or reactions to social media posts. In 2017, eight years after the United Airlines guitar handling debacle, it made headlines again when video footage was posted on social media showing passenger Dr. David Dao being forcibly dragged, screaming and bleeding, from United Express Flight 3411, so that a United Airlines staff person could take his legitimately booked seat instead. Unsurprisingly, outrage ensued online.

Aside from these public relations social media disasters, within the boundaries of the firm, there are plenty of dark side examples, too. Employers monitor their employees' activities on social media, disgruntled employees cause damage to employers' public reputation when they rant about their experiences, co-workers bully each other, and misinformation and aggressive social engagement cause work-tension. "Enterprise social media" platforms (e.g., Microsoft's *Yammer*, Salesforce's *Chatter*, or the collaboration tool *Slack*) are developed and deployed specifically to connect colleagues. However, despite the many knowledge management advantages these tools offer, they are not immune to these interpersonal ills either.

While media keep improving, our social behavior online seems to stagnate, at best. It sometimes even seems that social media are destroying many of the human traits that made us a social species in the first place. Firms wanting to avoid some of the social media risks will find a useful tool in the honeycomb framework. By analyzing the seven building blocks — conversations, sharing, presence, relationships, reputation, groups, and identity — they can monitor and understand the dark side that social media can present for their brands, customers, and workforce. However, much more work is necessary to improve the way we use social media. We hope that this article motivates our readers (as researchers, managers, employees, and social media consumers) to spend more time on understanding the dark side and weighing the long-term costs of using social media. A lot is at stake, and it's serious!

References

Alexa Internet. (2018). *The top 500 sites on the web*. Retrieved from https://www.alexa.com/topsites Accessed 22 May 2018.

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *The Journal of Economic Perspectives, 31*(2), 211—236.

van Alsenoy, B., Verdoodt, V., Heyman, R., Wauters, E., Ausloos, J., & Acar, G. (2015). *From social media service to advertising network: A critical analysis of Facebook's revised policies and terms*.

Beaver, G., & Jennings, P. (2005). Competitive advantage and entrepreneurial power: The dark side of entrepreneurship. *Journal of Small Business and Enterprise Development, 12*(1), 9—23.

Bennett, S., Maton, K., & Kervin, L. (2008). The 'digital natives' debate: A critical review of the evidence. *British Journal of Educational Technology, 39*(5), 775—786.

Berthon, P., Pitt, L., Kietzmann, J., & McCarthy, I. P. (2015). CGIP: Managing consumer-generated intellectual property. *California Management Review, 57*(4), 43—62.

Blackwell, D., Leaman, C., Tramposch, R., Osborne, C., & Liss, M. (2017). Extraversion, neuroticism, attachment style and fear of missing out as predictors of social media use and addiction. *Personality and Individual Differences, 116*, 69—72.

Brewer, M. B. (1999). The psychology of prejudice: Ingroup love and outgroup hate? *Journal of Social Issues, 55*(3), 429—444.

Buckels, E. E., Trapnell, P. D., & Paulhus, D. L. (2014). Trolls just want to have fun. *Personality and Individual Differences, 67*, 97—102.

Chang, J., Lefferman, J., & Pedersen, C. (2016). *When fake news stories make real news headlines*. abc News. Retrieved from https://abcnews.go.com/Technology/fake-news-stories-make-real-news-headlines/story?id=43845383 Accessed 15 June 2018.

Chou, H. T. G., & Edge, N. (2012). "They are happier and having better lives than I am": The impact of using Facebook on perceptions of others' lives. *Cyberpsychology, Behavior, and Social Networking, 15*(2), 117—121.

Cipriani, J. (2012). *How to prevent Facebook Messenger from sharing your location*. Retrieved from https://www.cnet.com/how-to/how-to-prevent-facebook-messenger-from-sharing-your-location Accessed 29 May 2018.

van Dijck, J. (2009). Users like you? Theorizing agency in user-generated content. *Media, Culture & Society, 31*(1), 41—58.

Eisenegger, M. (2009). Trust and reputation in the age of globalisation. In J. Klewes, & R. Wreschniok (Eds.), *Reputation Capital: Building and maintaining trust in the 21st century* (pp. 11—22). Berlin Heidelberg: Springer.

Elaluf-Calderwood, S., Kietzmann, J., & Saccol, A. Z. (2005). Methodological approach for mobile studies: Empirical research considerations. In *4th European conference on research methodology for business and management studies* (pp. 133—140).

Epstein, R. (2007). From Russia, with love. *Scientific American Mind, 18*(5), 16—17.

European Commission. (2018). *Final report of the high level expert group on fake news and online disinformation*. Retrieved from https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation Accessed 05 March 2018.

Eurostat. (2017a). *Digital economy and society in the EU*. Retrieved from http://ec.europa.eu/eurostat/cache/infographs/ict/images/pdf/pdf-digital-eurostat-2017.pdf Accessed 06 March 2018.

Eurostat. (2017b). *Social media — statistics on the use by enterprises*. Retrieved from http://ec.europa.eu/eurostat/statistics-explained/index.php/Social_media_-_statistics_on_the_use_by_enterprises#Further_Eurostat_information Accessed 22 May 2018.

Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. *Communications of the ACM, 59*(7), 96—104.

Fox, J., & Moreland, J. J. (2015). The dark side of social networking sites: An exploration of the relational and psychological stressors associated with Facebook use and affordances. *Computers in Human Behavior, 45*, 168—176.

Fuchs, C. (2014). Social media and the public sphere. *tripleC: Communication, Capitalism & Critique, 12*(1), 57—101.

Gupta, S. (2016). *Trump supporters call to boycott Pepsi over comments the CEO never made*. CNN Money. Retrieved from http://money.cnn.com/2016/11/16/news/companies/pepsi-fake-news-boycott-trump Accessed 17 June 2018.

Hannah, D. R., McCarthy, I. P., & Kietzmann, J. (2015). We're leaking, and everything's fine: How and why companies deliberately leak secrets. *Business Horizons, 58*(6), 659—667.

Hardaker, C. (2010). Trolling in asynchronous computer-mediated communication:

From user discussions to academic definitions. *Journal of Politeness Research, 6*(2), 215—242.

Hogg, M. A., & Reid, S. A. (2006). Social identity, self-categorization, and the communication of group norms. *Communication Theory, 16*(1), 7—30.

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! the challenges and opportunities of social media. *Business Horizons, 53*(1), 59—68.

Karl, K., Peluchette, J., & Schlaegel, C. (2010). Who's posting Facebook faux pas? A cross-cultural examination of personality differences. *International Journal of Selection and Assessment, 18*(2), 174—186.

Kietzmann, J. H. (2017). Crowdsourcing: A revised definition and introduction to new research. *Business Horizons, 60*(2), 151—153.

Kietzmann, J. H., Hermkens, K., McCarthy, I. P., & Silvestre, B. S. (2011). Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons, 54*(3), 241—251.

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin, 140*(4), 1073—1137.

Kumar, A., Bezawada, R., Rishika, R., Janakiraman, R., & Kannan, P. K. (2016). From social to Sale: The effects of firm generated content in social media on customer behavior. *Journal of Marketing, 80*(1), 7—25.

Kwan, G. C. E., & Skoric, M. M. (2013). Facebook bullying: An extension of battles in school. *Computers in Human Behavior, 29*(1), 16—25.

Lessig, L. (2008). In defense of piracy. *The Wall Street Journal.* Retrieved from https://www.wsj.com/articles/SB122367645363324303 Accessed 29 May 2018.

Levenson, J. C., Shensa, A., Sidani, J. E., Colditz, J. B., & Primack, B. A. (2016). The association between social media use and sleep disturbance among young adults. *Preventive Medicine, 85*, 36—41.

Livingstone, S., Kirwil, L., Ponte, C., & Staksrud, E. (2014). In their own words: What bothers children online? *European Journal of Communication, 29*(3), 271—288.

Lyndon, A., Bonds-Raacke, J., & Cratty, A. D. (2011). College students' Facebook stalking of ex-partners. *Cyberpsychology, Behavior, and Social Networking, 14*(12), 711—716.

Madden, M., & Smith, A. (2010). *Reputation Management and Social Media - how people monitor their identity and search for others online. Washington, D.C.* Retrieved from Pew Internet & American Life Project website: http://www.pewinternet.org/files/old-media/Files/Reports/2010/PIP_Reputation_Management_with_topline.pdf.

Malhotra, A., & van Alstyne, M. (2014). The dark side of the sharing economy and how to lighten it. *Communications of the ACM, 57*(11), 24—27.

Mander, J. (2017). *Daily time spent on social networks rises to over 2 hours.* Retrieved from https://blog.globalwebindex.com/chart-of-the-day/daily-time-spent-on-social-networks Accessed 10 June 2018.

Moorhead, S. A., Hazlett, D. E., Harrison, L., Carroll, J. K., Irwin, A., & Hoving, C. (2013). A new dimension of health care: Systematic review of the uses, benefits, and limitations of social media for health communication. *Journal of Medical Internet Research, 15*(4).

Naylor, R., Lamberton, C., & West, P. (2012). Beyond the "like" button: The impact of mere virtual presence on brand evaluations and purchase intentions in social media settings. *Journal of Marketing, 76*(6), 105—120.

News, B. B. C. (2013). *Reddit apologises for online Boston 'witch hunt'.* Retrieved from http://www.bbc.com/news/technology-22263020 Accessed 28 May 2018.

Nosouhi, M. R., Qu, Y., Yu, S., Xiang, Y., & Manuel, D. (2017). Distance-based location privacy protection in social networks. In *Telecommunication networks and applications conference (ITNAC)*, (pp. 1—6).

O'Keeffe, G., & Clarke-Pearson, K. (2011). Clinical report - the impact of social media on children, adolescents, and families. *Pediatrics, 127*, 800—804.

Pai, P., & Arnott, D. C. (2013). User adoption of social networking sites: Eliciting uses and gratifications through a means-end approach. *Computers in Human Behavior, 29*(3), 1039—1053.

Paniagua, J., Korzynski, P., & Mas-Tur, A. (2017). Crossing borders with social media: Online social networks and FDI. *European Management Journal, 35*(3), 314—326.

Park, N., Kee, K. F., & Valenzuela, S. (2009). Being immersed in social networking environment: Facebook groups, uses and gratifications, and social outcomes. *CyberPsychology and Behavior, 12*(6), 729—733.

Pfeffer, J., Zorbach, T., & Carley, K. M. (2014). Understanding online firestorms: Negative word-of-mouth dynamics in social media networks. *Journal of Marketing Communications, 20*(1—2), 117—128.

Przybylski, A. K., Murayama, K., Dehaan, C. R., & Gladwell, V. (2013). Motivational, emotional, and behavioral correlates of fear of missing out. *Computers in Human Behavior, 29*, 1841—1848.

Raskauskas, J., & Stoltz, A. D. (2007). Involvement in traditional and electronic bullying among adolescents. *Developmental Psychology, 43*(3), 564—575.

Roulin, N. (2014). The influence of employers' use of social networking websites in selection, online self-promotion, and personality on the likelihood of faux pas postings. *International Journal of Selection and Assessment, 22*(1), 80—87.

Sabate, F., Berbegal-Mirabent, J., Cañabate, A., & Lebherz, P. R. (2014). Factors influencing popularity of branded content in Facebook fan pages. *European Management Journal, 32*(6), 1001—1011.

Scharfstein, D. S., & Stein, J. C. (2000). The dark side of internal capital markets: Divisional rent-seeking and inefficient investment. *The Journal of Finance, 55*(6), 2537—2564.

Scheiner, C. W., Krämer, K., & Baccarella, C. V. (2016). Cruel Intentions? — the role of moral awareness, moral disengagement, and regulatory focus in the unethical use of social media by entrepreneurs. *Lecture Notes in Computer Science, 9742*, 437—448.

Schlosser, E. (2002). *Fast food nation: The dark side of the all-American meal.* Boston, MA: Houghton Mifflin Harcourt.

Schmidt, G. B., & O'Connor, K. W. (2015). Fired for Facebook: Using NLRB guidance to craft appropriate social media policies. *Business Horizons, 58*(5), 571—579.

Smith, A. N., Fischer, E., & Yongjian, C. (2012). How does brand-related user-generated content differ across YouTube, Facebook, and Twitter? *Journal of Interactive Marketing, 26*(2), 102—113.

Suran, M., & Kilgo, D. K. (2017). Freedom from the press? How anonymous gate-keepers on Reddit covered the Boston Marathon bombing. *Journalism Studies, 18*(8), 1035—1051.

Tajfel, H., & Turner, J. C. (2004). The social identity theory of intergroup behavior. In J. T. Jost, & J. Sidanius (Eds.), *Political Psychology: Key readings (key readings in social Psychology)* (pp. 276—293). New York, NY: Psychology Press.

The Children's Society. (2018). *Safety Net: Cyberbullying's impact on young people's mental health.*

Wagner, T. F. (2017). Promoting technological innovations: Towards an integration of traditional and social media communication channels. *Lecture Notes in Computer Science, 10282*, 256—273.

Wagner, T. F., Baccarella, C. V., & Voigt, K.-I. (2017). Framing social media communication: Investigating the effects of brand post appeals on user interaction. *European Management Journal, 35*(5), 606—616.

Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P. G., & Cranor, L. (2011). I regretted the minute I pressed share: A qualitative study of regrets on Facebook. In *Proceedings of the 7th symposium on usable privacy and security* (Vol. 10).

Wilson, M., Robson, K., & Botha, E. (2017). Crowdsourcing in a time of empowered stakeholders: Lessons from crowdsourcing campaigns. *Business Horizons, 60*(2), 247—253.

Wolak, J., Liberatore, M., & Levine, B. N. (2014). Measuring a year of child pornography trafficking by US computers on a peer-to-peer network. *Child Abuse & Neglect, 38*(2), 347—356.

Wolf, M. J., Miller, K., & Grodzinsky, F. S. (2017). Why we should have seen that coming: Comments on Microsoft's tay experiment, and wider implications. *ACM SIGCAS - Computers and Society, 47*(3), 54—64.

Wong, J. C. (2017). Former Facebook executive: Social media is ripping society apart. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2017/dec/11/facebook-former-executive-ripping-society-apart Accessed 02 May 2018.

Woodruff, A. (2014). Necessary, unpleasant, and disempowering: Reputation management in the internet age. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 149—158).

Zhou, L., & Wang, T. (2014). Social media: A new vehicle for city marketing in China. *Cities, 37*, 27—32.

van Zoonen, W., Verhoeven, J. W., & Vliegenthart, R. (2017). Understanding the consequences of public social media use for work. *European Management Journal, 35*(5), 595—605.