Check for updates

Received: 29 October 2020 | Revised: 16 June 2021 | Accepted: 18 June 2021

DOI: 10.1002/mar.21542

RESEARCH ARTICLE

Psychology & Marketing WILEY

Words matter: How privacy concerns and conspiracy theories spread on twitter

Marco Visentin[1] | Annamaria Tuan[1] | Giandomenico Di Domenico[2]

[1]Department of Management, University of Bologna, Bologna, Italy

[2]Faculty of Business and Law, University of Portsmouth, Portsmouth, UK

Correspondence

Marco Visentin, Department of Management, University of Bologna, via Capo di Lucca 34, Bologna.
Email: marco.visentin@unibo.it

Abstract

The use of contact-tracing apps to curb the spreading of the COVID-19 pandemic has stimulated social media debates on consumers' privacy concerns about the use and storage of sensitive data and on conspiracy theories positing that these apps are part of plans against individuals' freedom. By analyzing the type of language of tweets, we found which words, linguistic style, and emotions conveyed by tweets are more likely to be associated with consumers' privacy concerns and conspiracy theories and how they affect virality. To do so, we analyze a set of 5615 tweets related to the Italian tracing app "Immuni". Results suggest that consumers' privacy concerns and conspiracy theories belong to different domains and exert different effects on the virality of tweets. Furthermore, the characteristics of the text (namely, complexity, certainty and emotions) cue different Twitter users' behaviors. This study helps researchers and managers to infer the psychological mechanisms that lead people to spread tweets about privacy concerns and conspiracy theories as well as how these texts impact the user who receives it.

KEYWORDS

conspiracy theory, consumer privacy, contact-tracing apps, privacy concerns, Twitter, virality

1 | INTRODUCTION

Social media have become powerful channels to freely interact with others (Appel et al., 2020). Thanks to social media users can easily grab the "megaphone" and attract attention, influencing other individuals (Hewett et al., 2016) as well as affecting companies' reputation (Herhausen et al., 2019). However, social media represent not only relevant platforms for individuals to express themselves (Choi & Sung, 2018) but they have also created the conditions for the propagation of problematic contents (Di Domenico & Visentin, 2020). As social media platforms are subject to limited governmental oversight regarding the collection and usage of users' data, social media users' privacy concerns have dramatically increased over the last years (Bright et al., 2021). In addition, recent data breach scandals have exacerbated this phenomenon (Hinds et al., 2020). Alongside this, social media have also become places where different types of misinformation can thrive (Allcott & Gentzkow, 2017; Appel et al., 2020). Among them, conspiracy theories have recently proliferated in digital environments, posing potentially serious threats to individuals' health (Douglas et al., 2017). The dissemination of these problematic contents online has further intensified during the pandemic. In particular, during the COVID-19 pandemic, various governments introduced contact-tracing apps, aimed at quickly identifying and informing users who may have come into contact with an infected person (Trang et al., 2020). The announcement of the

This study did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

This is an open access article under the terms of the Creative Commons Attribution-NonCommercial-NoDerivs License, which permits use and distribution in any medium, provided the original work is properly cited, the use is non-commercial and no modifications or adaptations are made.
© 2021 The Authors. *Psychology & Marketing* published by Wiley Periodicals LLC

release of tracing apps has stimulated the proliferation of problematic contents on social media regarding their actual benefits, focusing the attention on consumers' *privacy concerns* about the use and storage of sensitive data (Maseeh et al., 2021; Miller & Abboud, 2020; Sweeney, 2020) and on *conspiracy theories* stating that these apps are part of plans against individuals' freedom (Appleby, 2020).

Given the timely debate, this topic is mainly discussed on websites or newspaper articles (e.g., Birnbaum & Spolar, 2020; Love, 2020) but academic literature is still scant, with limited exceptions from other fields of study (e.g. Amann et al., 2021; Sweeney, 2020). In fact, marketing literature lacks the understanding of the influence of *privacy concerns* and *conspiracy theories* on virality both from a linguistic and content perspective. This paper fills this gap by analysing *how* social media users express their *privacy concerns* and *conspiracy theories* on these platforms and *how much* these contents increase the virality of social media posts.

In digital environments, users' interactions with contents are indeed gauged through virality metrics (e.g., "likes", "retweets" and "shares"), which are employed as key indicators of engagement and attitudes toward the content (Peters et al., 2013). Thus, marketing interest in understanding why and how different contents achieve virality has steadily increased over the last years. Past research on this topic has mainly focused on two areas. First, research has analysed language characteristics of contents as drivers of virality. Language plays a critical role in social interactions given that people usually use cues to understand and to develop impressions of others (Xu & Zhang, 2018). In fact, individuals' personality traits (Hirsh & Peterson, 2009), identities (McAdams, 2001), and emotional states (Tausczik & Pennebaker, 2010) are reflected by their use of words. Recently, marketing research has started to focus on the influence of the linguistic style of texts on social media virality, focusing on the usage of function words (Aleti et al., 2019), pronoun choices (Labrecque et al., 2020) and the narrative style of texts (Van Laer et al., 2019).

Secondly, past scholarship has also focused on the content itself. A growing body of literature has investigated which types of contents drive more virality, in terms of emotional (Akpinar & Berger, 2017), informative (Berger & Milkman, 2012), and commercial (Tellis et al., 2019). More recently, as misinformation has become a pervasive phenomenon in digital environments (Di Domenico et al., 2021), academics have started to devote attention to this topic, analysing the spreading patterns of fake news and how it goes viral (e.g., Vosoughi, Roy & Aral, 2018; Vicario et al., 2019). However, to the best of our knowledge, research about how problematic contents and their linguistic characteristics influence virality is still limited.

Our study focuses on Twitter, which is a micro-blogging social network that facilitates a quick spread of information by using the retweet function (Colleoni et al., 2014; Kietzmann et al., 2011; Lamberton & Stephen, 2016). Since the text reported in tweets is an invaluable source to detect what people wants to convey with a text and how it affects others (e.g., Berger et al., 2020), we focus on the language used by Twitter users. Thus, we analyze a set of 5615 tweets around the Italian "Immuni" contact-tracing app, in two studies. Study 1 aims at performing an analysis of consumers' *privacy concerns* regarding the app's adoption and its related *conspiracy theories*. Given the absence of specific categories for *privacy concerns* and *conspiracy theories*, we created and validated two custom dictionaries (in the Italian language) and conducted the analysis using the LIWC software (Pennebaker et al., 2007). Study 2 aims at identifying the tweets characteristics (i.e., *privacy concerns*, *conspiracy theories*, *linguistic style* and *emotions*) that drive tweets' virality, in terms of the number of retweets. To account for the linguistic style and for emotions, we used the Italian language translation of the dictionaries included in the LIWC software (Agosti & Rellini, 2007).

Our research contributes to both theory and practice in different ways. First, this study contributes to the growing body of literature which focuses on how users build meanings of their concerns on social media and how they affect the audience (e.g., Aleti et al., 2019; Berger et al., 2020; Netzer et al., 2019). Extant privacy research has mainly focused on measuring consumers' privacy concerns and their effects on social media behaviours (Baruh et al., 2017; Chen & Kim, 2013; Jeong & Kim, 2017), information disclosure (Blose et al., 2020; Shin & Kang, 2016) and mobile technologies adoption (Harris et al., 2016). Moreover, considerable research has focused on the *privacy paradox* (Kokolakis, 2017), attempting to explain the ambiguous discrepancy between privacy attitudes and online behaviors (Dienlin & Trepte, 2015; Gerber et al., 2018). In this study, we undertake another perspective and build a comprehensive custom dictionary for both *privacy concerns* and *conspiracy theories* that could serve as a powerful tool for identifying these topics of discussion on social media. Second, we provide an understanding of how consumers express their privacy and conspiracy concerns relating to technologies (Plangger & Montecchi, 2020), also evaluating which content and linguistic characteristics are more likely to drive contents' virality on Twitter. Specifically, we focus on (1) the topic of the tweets, in terms of consumers' privacy concerns and conspiracy theories, (2) the linguistic complexity of the tweets, and (3) the presence of certainty in language and 4) the presence of positive and negative emotions.

The remainder of the paper is structured as follows. Section 2 depicts our theoretical framework and hypotheses development. Then, in Section 3 we outline our empirical analysis and in Section 4 we provide theoretical contributions as well as managerial implications of the study.

2 | THEORETICAL FRAMEWORK AND HYPOTHESES DEVELOPMENT

The analysis of the linguistic drivers of *privacy concerns* on Twitter, relative to data disclosure using contact-tracing apps, could not disregard the simultaneous surge of *conspiracy theories* about the virus proliferated on social media (Georgiou et al., 2020). These theories range from unconfirmed explanations of the emergence of the virus; the development of bio-weapons; the role of 5 G technology in spreading the virus and, together with contact-tracing apps, in manipulating people. Said theories suggest that the world is ruled by small elites (van Prooijen, 2018) whose intrusion into people's lives comes with a high likelihood of breaches of privacy (Backhouse & Halperin, 2008). Thus, the pandemic has put the abiding debate around surveillance and privacy in digital tool development under the spotlight so that when this surveillance is alleged to be part of secrets plans to control people, *privacy concerns* are expressed more intensely (Degirmenci, 2020; Gu et al., 2017).

Previous literature suggests that in highly stressful situations, individuals may experience "hypervigilance", a behavior characterized by elevated arousal, anxiety, and desire to obtain information about the causes of the stressful event (Rehman et al., 2020; Van Prooijen & Jostmann, 2013; Van Prooijen, 2018). In the COVID-19 context, hypervigilance might have manifested in the form of increased consumers' *privacy concerns* related to the adoption of contact-tracing apps, leading individuals to manifest their concerns on social media and avoid apps usage.

In addition, it becomes relevant analysing how these constructs spread online in a platform like Twitter, which represents one of the major platforms used by people to debate about extant problems (Kietzmann et al., 2011, Rust et al., 2021). Understanding the origins, the features and the evolution of viral misinformation is a key function of social media surveillance (Di Domenico et al., 2021), and timely research is needed to combat misinformation's spread (Ahmed et al., 2020; Chang et al., 2020; Chou et al., 2018).

In this line, the words and the writing styles we use are indicative of our psychological mechanisms and discover our personality (Berger et al., 2020; Humphreys & Wang, 2018; Netzer et al., 2019; Pennebaker et al. 2010). In fact, not only the content (*what we say*) but also the linguistic style (*how we say*) reveals how people construe the world around them and affects the audience (e.g., Aleti et al., 2019; Bertele et al., 2020).

Previous literature has widely investigated which type of content influence retweet rates (e.g., Hollebeek & Macky, 2019; Lee et al., 2018) and, more recently, marketing scholars have started to focus on the role of the linguistic features of a tweet in affecting retweets (e.g., Aleti et al., 2019, Cruz et al., 2017; Pezzuti et al., 2021). Meanwhile, scant literature has focused on how users communicate on Twitter and how they can influence their peers. Linguistic style indeed can reveal attempts at managing impressions and relationships more accurately than the content because the former is usually not under conscious control (Ludwig et al., 2013; Pennebaker et al., 2003).

Consistently, our first focus of analysis emphasizes the tweets' *topic*, namely the presence of *privacy concerns* and *conspiracy theories*. Following prior research (Aleti et al., 2019; Hollebeek & Macky, 2019; Pezzuti et al., 2021) our second focus concerns the *linguistic style* of tweets, including the effect of *tweets complexity* and the presence of *certainty in language* on retweet rates. Finally, our third focus of analysis revolves around *emotions*, as emotional language was found to play an important role in determining the virality of contents (Berger & Milkman, 2012; Xu & Zhang, 2018). Figure 1 shows the theoretical framework for this study.

2.1 | Tweets' topic

2.1.1 | Privacy concerns

In nowadays information age, retailers, manufacturers, service providers, and non-profit organizations routinely collect and use detailed consumer information (Bright et al., 2021; Maseeh et al., 2021). These "vertical dynamics" of information, while providing valuable insights for institutions' commercial interests (Bazarova & Masur, 2020), have made privacy one of the most important ethical issues of our time (Pizzi & Scarpi, 2020; Plangger & Montecchi, 2020; Shilton & Greene, 2019).

As the concept of privacy is multidimensional, its evaluation depends on the measurement of different privacy-related variables, which can be quantified. Among them, *privacy concerns* has been widely adopted as a central construct in privacy research (Smith et al., 2011). Online privacy concerns "represent how much an individual is motivated to focus on his or her control over a voluntary withdrawal from other people or societal institutions on the Internet, accompanied by an uneasy feeling that his or her privacy might be threatened" (Dienlin et al., 2019; p. 7). Thus, central to this concept is the ability or desire for individuals to exercise a form of control over

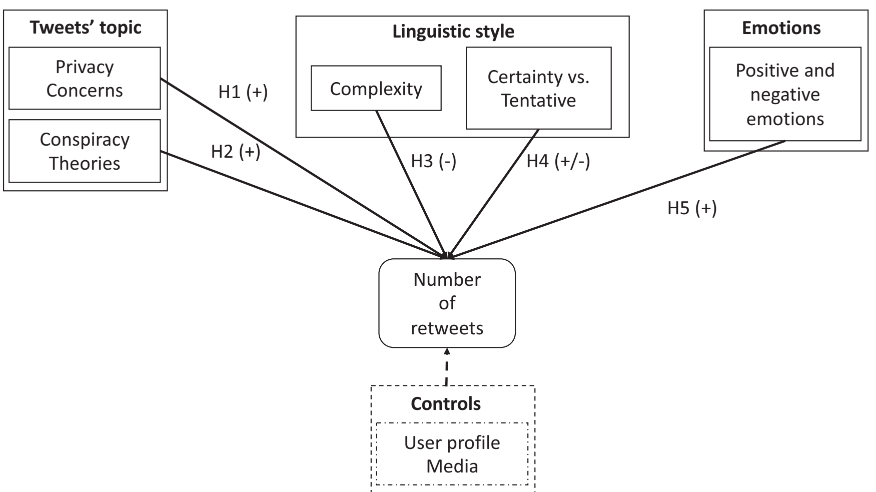


FIGURE 1 Theoretical framework

who has access to personal data (i.e., disclosure), how personal data are used (i.e., appropriation and false light), and what volume of advertising and marketing offers arises from the use of personal data (i.e., intrusion) (Osatuyi, 2015; Plangger & Montecchi, 2020). In the nowadays data-driven world, information disclosure is a fundamental part of the functioning of e-commerce (Maseeh et al., 2021), social network services (Shibchurn & Yan, 2015), location-based services (Zhao, Lu and Gupta, 2012) and mobile apps (Gu et al., 2017). One major consequence of consumers' *privacy concerns* is that they can obstacle the disclosure of information on these online environments (Bright et al., 2021).

We expect that social media users are likely to share digital contents featuring privacy concerns for what concerns, in general, represent, that is an increased attention (to a specific topic) and a negatively valenced emotion (Dienlin et al., 2019).

First, the risks related to the disclosure of information might lead users to express their *privacy concerns* through social media platforms, in a bid to inform other users about possible privacy threats associated with the usage of products and services (Rehman et al., 2020). In doing so, a user strives to impact her followers' minds and behaviours (Rudat et al., 2014) by galvanizing the lack of transparency in the information related to the topic. The COVID crisis has proven to be a highly stressful situation having a destructive impact on people wellbeing, leading to increased perceptions of hypervigilance (Georgiou et al., 2020; Vanhaecht et al., 2020). When in the hypervigilant state, people show an increased suspicion and attention towards the possible malevolent actions of other people or institutions (Van Prooijen & Jostmann, 2013), and thus heightened concerns. As a consequence, consumers' feeling of suspicion are likely to elicit the retransmission of privacy concerns on social media, in a way to alert other users about possible threats associated with data usage.

Secondly, as concerns intrinsically represent negative feelings (Dienlin et al., 2019), their negative valence facilitates the spreading of these contents on social media. Within the news domain, Hansen et al. (2011) found that negative news contents are retweeted more than positive news on Twitter. This is especially true during times of crises (Xu & Zhang, 2018) and disasters (Chen & Sakamoto, 2014). Moreover, negative eWOM is associated with greater virality in online brand communities (Herhausen et al., 2019).

Therefore, we hypothesize that the spread of a tweet is positively affected by the number of words belonging to *privacy concerns* for what a concern intrinsically represents (i.e., increased attention and negative emotions). Formally:

H1: *The likelihood of a tweet to be retweeted is positively affected by the number of words associated with privacy concerns.*

2.1.2 | Conspiracy theories

Conspiracy theories, proliferating in social and political discourse (Douglas et al., 2017), represent attempts to provide explanations for important events that involve secret plots by powerful and malevolent groups (Byford, 2011; van Prooijen, 2018). *Conspiracy theories* fulfil epistemic motives because people need to find causal explanations for events where available information is conflicting or for finding meaning when the events seem random (Douglas et al., 2017). Causal explanations also serve the need for people to feel secure in the environment and to exert control over it (Tetlock, 2002). *Conspiracy theories* may promise to make people feel safer as a form of cheater detection, in which dangerous and untrustworthy individuals are recognized and the threat they pose is reduced or neutralized (Bost & Prunier, 2013). Conspiracy explanations are also informed by social motivations such as the desire to belong and maintain a positive image of the self and the in-group, (Douglas et al., 2017) by blaming the out-groups for negative outcomes (Cichoka et al., 2016). Interestingly, social media collaborative filtering algorithms have enabled the creation of so-called echo chambers (Quattrociocchi et al., 2016) where the spreading of *conspiracy theories* thrives (Del Vicario et al., 2016).

The COVID-19 pandemic would appear to be a situation that facilitates the spread of misinformation and *conspiracy theories* at an unprecedented scale and pace (Cuan-Baltazar et al., 2020; Di Domenico & Visentin, 2020; Fisher, 2020), leading many to refer to this mis- and disinformation crisis as a "misinfodemic", defined as the "viral spread of false information" (McGinty & Gyenes, 2020). This is because the situation is highly stressful for individuals, and it leads to uncertainty about the limits and appropriateness of governments actions. Moreover, previous research has shown how situational threats and crises can foster conspiracy beliefs (Mashuri & Zaduqisti, 2014; van Proijen & Douglas, 2017).

Recently, Gruzd and Mai (2020) analyzed the spread of the conspiracy campaign #Filmyourhospital in the United States, a hashtag used on Twitter to engage people to take pictures and videos of empty hospitals to "prove" that the COVID-19 pandemic is an elaborate hoax. Another example is the spread on Twitter of tweets about "plandemic" (e.g., #plandemic)—the notion that the COVID-19 pandemic was planned or fraudulent—which fueled the flow of several distinct *conspiracy theories* related to COVID-19 and misinformation (Kearney et al., 2020). Hence, during the COVID-19 pandemic, we have assisted to a surge in the proliferation of Covid-related *conspiracy theories* on Twitter, some of them targeting also contact-tracing apps with the aim to run against the governments and the small elites. From the non-existent "FEMA camps" to theories describing the apps as a part of a plot by secret global elites, the engagement on social media of these theories has steadily increased (Appleby, 2020; Gruzd & Mai, 2020).

Consequently, we hypothesize that the spread of a tweet is positively affected by the number of words that express *conspiracy theories*. Formally:

H2: *The likelihood of a tweet to be retweeted is positively affected by the number of words associated with conspiracy theories.*

2.2 | The linguistic style of a tweet

2.2.1 | Complexity of the language

Every text may convey a simple or a complex style of language (Tausczik & Pennebaker, 2010). This is also the case of tweets, even though they are typically short (Kietzman et al., 2011). In the context of deceptive speech, users tend to speak and write in a less complex way, by reducing the *number of words*, by using fewer *propositions*, less *long* words and less words related to *cognitive mechanisms* (words such as *think, know, question)* (Tausczik & Pennebaker, 2010). Text *complexity* indeed may be reduced in deceptive speech because of the cognitive load required to maintain a story that is contrary to experience, and the effort needed to try to convince others that something false is true. Even though previous literature fails in providing some empirical support or direct causalities between text complexity and positive behaviours towards it, we can argue that the more a text is complex, the less it will be convincing and that, in turn, this text will be shared less. We can therefore expect that Twitter users crafting *privacy concerns* and/or *conspiracy theories* in a tweet by using complex periphrases would limit the virality of their tweets.

These speculations converge to the following hypothesis:

H3: *The likelihood of a tweet to be retweeted is negatively affected by (H3a) the number of words, (H3b) the density of prepositions, (H3c) the density of words with more than six letters, (H3d) the density of words associated with cognitive mechanisms.*

2.2.2 | Certainty in language

Certainty is defined as "the state of being completely confident or having no doubt about something" (Cambridge, 2020), thus referring to a sense of conviction or a general air of confidence that characterizes language. Words that communicate certainty usually connote totality and completeness (entire, everywhere, wholly), conviction (commitment, definite, fact, obvious), and permanence (forever, always).

When brand messages on social media use certainty in language, they are associated with higher levels of consumer engagement than when using tentative language (Pezzutti, Leonhard & Warren, 2021; Also, Leek et al., 2019). From the point of view of the individual, a post using words expressing certainty appears more powerful than a post using tentative words (Hart & Childers, 2004; Hart et al., 2009). Moreover, power is associated with desirable characteristics such as prestige and status, and it stimulates consumers attention (Billett et al., 2014; Bryan et al., 2011). In the case of *privacy concerns* or *conspiracy theories*, we can hypothesize that users strive to show their power against small elites who might breach their privacy by using certainty in language rather than tentativeness (Backhouse & Halperin, 2008; van Prooijen, 2018). Thus, we can hypothesize that using certainty versus tentativeness in tweets featuring *privacy concerns* or *conspiracy theories* stimulates virality. Formally:

H4: *The likelihood of a tweet to be retweeted is positively affected by (H4a) the density of words expressing certainty and it is negatively affected by (H4b) the density of words expressing tentativeness.*

2.3 | Emotions

The marketing literature converges on the importance of emotions for individuals' evaluations and behaviors (e.g., Pedersen, 2021; Rust et al., 2021). In turn, either positive (e.g., "happy", "fantastic") or negative emotions (e.g., "sad", "awful") may be stimulated by emotion-focused contents (Tellis et al., 2019). Moreover, literature suggests that highly emotional content is more likely to be shared frequently and widely since the audience is more receptive to a message when it arouses affective states (Akpinar & Berger, 2017; Rimé, 2009; Villarroel Ordenes et al., 2017; Xu & Zhang, 2018). Akpinar and Berger (2017), for instance, studied the effect of information- versus emotion-focused ads on sharing, finding that the latter induce more sharing intentions. These findings are also supported by Nikolinakou and King (2018) who found that in video advertising, content-specific positive emotions act as triggers for sharing expressions in social media. In the context of Twitter, tweets with highly positive emotions as well as tweet with highly negative emotions are more likely to be shared than neutral tweets (Hansen et al., 2011; Keib et al., 2018).

Consistently, we may expect that tweets related to *privacy concerns* and *conspiracy theories* will be more shared in the case of highly emotional texts rather than texts only presenting facts. More in detail:

H5: *The likelihood of a tweet to be retweeted is positively affected by the density of (H5a) positive emotions and (H5b) negative emotions.*

2.4 | Control variables

In addition to our hypotheses, we include in our analysis some control variables from past research.

Previous literature suggests that the *number of followers*, the *number of friends* and the volume of *statuses* provide information about the user profile in terms of authority and it acts as a straightforward indicator of source influence (Xu & Zhang, 2018).

Moreover, non-textual characteristics of a tweet can act as relevant cues leading to its diffusion on Twitter. Previous literature suggests that vividness and interactivity influence virality (De Vries et al., 2012; Tellis et al., 2019). In particular, the vividness of a tweet entails the presence of *images* while its interactivity requires the link to some external source, that is an *url*.

3 | EMPIRICAL ANALYSIS

In Study 1 we: (1) developed a custom dictionary related to *privacy concerns* and a custom dictionary related to *conspiracy theories*; (2) manually coded tweets to scrutinize whether they were related to *privacy concerns* or *conspiracy theories*; and (3) tested the predictive ability of the dictionary to correctly classify tweets. In Study 2 we empirically assessed the effect of *privacy concerns* and *conspiracy theories* on the ability of a tweet to be retweeted.

Data includes 5615 tweets retrieved basing on the hashtags #immuni #immuniapp, and the keywords "immuni AND app", "covid AND app", "covid AND privacy", "immuni AND privacy". Data collection was performed in July 2020. From the initial set of tweets, we removed retweets and tweets from verified users.

3.1 | Study 1: Building and validating the two custom dictionaries

To capture *privacy concerns* and *conspiracy theories*, we created two custom dictionaries (Pennebaker, Francis, & Booth, 2007). In the development of the dictionaries, we followed the procedure suggested by Humphreys and Wang (2018) (see Table 1).

Dictionary creation. First, we randomly sampled 523 tweets from our data set (about 10% of the total). Second, authors read and coded the tweets according to the procedures outlined by Corbin and Strauss (2014) to develop categories for customized analysis: following a grounded theory approach (Morse et al., 2002), each coder suggested a words list (i.e. open coding), resulting in 275 words, which were then grouped into 3 broader categories (i.e. axial coding), namely *privacy concerns*, *conspiracy theories*, *both privacy and conspiracy*. To avoid false positives and negatives, we added all the relevant synonyms, word stems, and tenses of the originally selected words to the original dictionary. This procedure provided 84 words for *privacy concerns*, 43 words for *conspiracy theories* and 51 words for *both privacy and conspiracy*.

Dictionary validation. To assess the dictionaries' construct validity, following Humphreys and Wang (2018), three external coders validated the dictionaries. They were instructed and provided with the definition of *privacy concerns* and *conspiracy theories* suggested by the literature (see Appendix A). They voted to either include or exclude a word from the category independently. Then, words have been included if two of the three coders voted to include it, otherwise, they were excluded from the category. This step led to the drop out of the *both privacy and conspiracy* category and it allowed us to retain 55 words in the *privacy concerns* category and 31 in the *conspiracy theories* category, leading to the definition of the *PrivacyDIC* and *ConspiracyDIC* dictionaries, respectively. Table 2 presents the two dictionaries (see Appendix B for the full list of words in Italian and English):

We finally included the two dictionaries *PrivacyDIC and ConspiracyDIC* in LIWC (Linguistic Inquiry and Word Count; Tausczik & Pennebaker, 2010) and performed the automated text analysis on the whole set of 5615 tweets. LIWC analyzes each post and finds target words one by one. For instance, if the tweet contains the word "cybersecurity" a match is recorded for the *privacy concern* category. Then, for each tweet, LIWC creates an output variable that reflects the number of words found in the tweet matching the category divided by the total number of words in the tweet (i.e., density). We also included in the analysis the LIWC categories related to *text complexity*, word count (*wordcount*), presence of prepositions (*prepositions*), words with more than six letters (*six letters*) and cognitive mechanisms (*cognitive mechanisms*). To account for *certainty in language*, we included words communicating tentativeness (*tentative*) and certainty (*certainty*). To account for *emotions*, we included negative and positive emotions (*negative emotions* and *positive emotions*, respectively). For these categories, we used the Italian translation of the LIWC dictionary (Agosti & Rellini, 2007).

Dictionary post-measurement validation. Construct validity of the privacy and conspiracy variables was assessed through manual coding. We first extracted a sub-sample of 30 tweets with high level of privacy (according to PrivacyDIC) a sub-sample of 30 tweets with high level of conspiracy (according to ConspiracyDIC). We considered "high-level" a rating greater than the 95% quantile of the distribution. Second, we

TABLE 1 Methodological steps

Data collection
Scraping of tweets with R (hashtags #immuni #immuniapp, keywords "immuni AND app", "covid AND app", "covid AND privacy", "immuni AND privacy")
Removed retweets and tweets from verified users
Final sample: 5617 tweets
Dictionary creation
Extraction of a random sub-sample (10% of sample tweets)
Authors identified words and categories related to privacy and conspiracy by using a bottom-up approach
Dictionaries contained: 84 words for *PrivacyDIC*, 43 for *ConspiracyDIC* and 51 for *Both Privacy and Conspiracy*
Dictionary validation
Three external coders evaluate the dictionary categories. If two out of three coders agree that the word is part of the category, include it otherwise exclude it.
Final dictionaries: 55 words for PrivacyDIC and 31 for ConspiracyDIC
Automated text analysis
Run LIWC on the 5617 tweets
Post-measurement validation
104 human coders validated results obtained from automated text analysis
Testing of the predictive power of the dictionaries through machine learning

TABLE 2 Privacy and conspiracy dictionary

Dictionary	n. of words	Example of words[a]
PrivacyDIC	55	Protection, register, position, policy
ConspiracyDIC	31	Fault, dictatorship, prohibition, freedom, invade, occupy

[a]original words are in Italian.

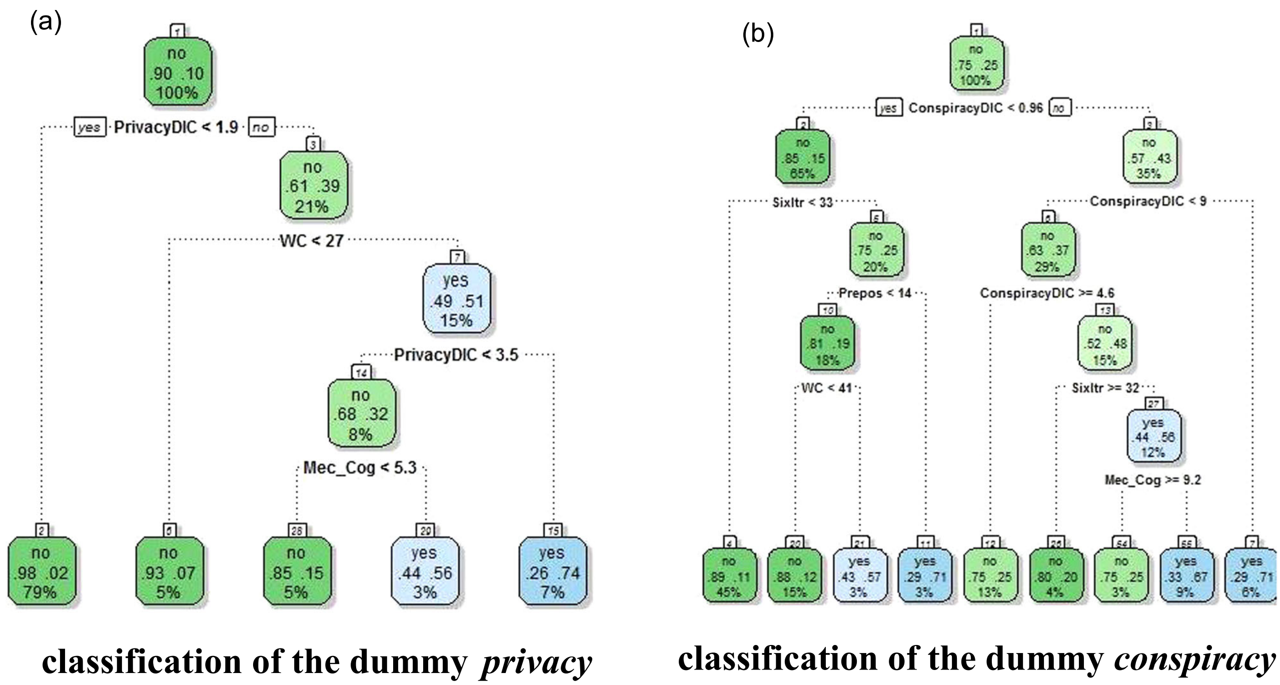


FIGURE 2 (a): classification of the dummy *privacy*. (b): classification of the dummy *conspiracy*

included the 60 (=30 + 30) tweets as long as 10 neutral tweets in a Qualtrics survey asking whether a tweet could be considered including privacy concerns or conspiracy theories. In the survey, for each tweet, we designed a specific page containing the criteria of Appendix A, and asking for a yes/no response. Given the high number of tweets, we designed a randomized assignment of tweets to each respondent. Third, we used a panel of about one hundred Italian-speaking participants from Prolific. We excluded the participants that did not pass a control check. Each one of the 104 participants evaluated 34.9 tweets on average (95% conf. interval: 29.8-39.8). We obtained an average level of agreement of .70% (95% conf. interval: .64 - .75) for the tweets containing privacy concerns according to our PrivacyDIC; and an average level of agreement of .85% (95% conf. interval: 0.82–0.89) for the tweets containing conspiracy theories according to our ConspiracyDIC. Consistent with Humpreys and Wang (2018) we concluded that the high level of agreement obtained between computer-coded results with human-coded results supports the validity of our PrivacyDIC and ConspiracyDIC.

Moreover, to further strengthen the external validity and replicability of PrivacyDIC and ConspiracyDIC, a supplementary study was carried out testing the power of the dictionaries on two different datasets. Details of this validity test can be found in Appendix C.

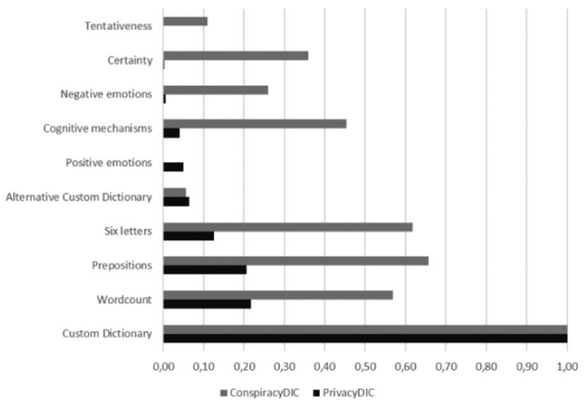
3.1.1 | Testing the predictive power of the dictionaries

In addition to the post-measurement validation, we also assess the extent to which *PrivacyDIC* and *ConspiracyDIC* are predictive of *privacy concerns* or *conspiracy theories*. Therefore, we relied on a machine learning approach based on pattern recognition (namely, *gradient boosting*, e.g.: Friedman, 2002). We adopted this approach since the language descriptors of a text provide a pattern, and we are interested in assessing the capability of *PrivayDIC* and *ConspiracyDIC* to prevail on the other descriptors in indicating the nature of the text analyzed.

First, the three authors individually classified the 523 tweets according to their *privacy concerns* and *conspiracy theories* inclusion on three-points Likert scales (1 = "no conspiracy/privacy at all", 2 = "indirect or partial mention to conspiracy/privacy", 3 = "full conspiracy/privacy content"). The definition of *privacy concerns* and *conspiracy theories* suggested by the literature guided the evaluation of the tweets (Appendix A). The Krippendorff's Alpha indicates a high level of agreement among coders ($\text{Alpha}_{\text{privacy}}$ = 0. 823, $\text{Alpha}_{\text{conspiracy}}$ = 0. 864). *Privacy concerns* and *conspiracy theories* display limited correlation (r = 0.276, p = .005). This procedure provided a dummy variable *privacy* and a dummy variable *conspiracy* (0 = "no"; 1 = "yes").

Second, we predictively classified the dummy *privacy* (Model 1) and the dummy *conspiracy* (Model 2). We used the 66% of classified tweets as the training set and the remaining 33% as the test set. We used the machine learning algorithm *gradientBoost* (*GRADIENT BOOSTing*; Natekin & Knoll, 2013; Ridgeway & Ridgeway, 2004; Friedman, 2002). This algorithm uses combinations of Classification And Regression Trees (CART; Friedman et al., 2000) as base classifiers, each obtained on a bootstrap replicate of the training set (e.g.: Friedman, 2002). Typical tree-models classifiers split each node based on the predictor that ensures the best reduction of variance (Figure 2 reports examples of CART for the *dummy* privacy and *conspiracy* respectively). Then, the classification is obtained by sequentially updating the current predictor with the under-fitted predictions, ensuring the errors made previously are corrected.

TABLE 3 Influence of *custom dictionary vs. other categories*



Category	Privacy Concerns	Conspiracy Theories
Custom Dictionary	1,00	1,00
Wordcount	0,22	0,57
Prepositions	0,21	0,66
Six letters	0,13	0,62
Alternative Custom Dictionary	0,06	0,06
Positive emotions	0,05	0,00
Cognitive mechanisms	0,04	0,45
Negative emotions	0,01	0,26
Certainty	0,00	0,36
Tentativeness	0,00	0,11

Note: in the case of Privacy Concerns, Custom Dictionary is *PrivacyDIC* and Alternative Custom Dictionary is *ConspiracyDIC;* in the case of Conspiracy Theories, Custom Dictionary is *ConspiracyDIC* and Alternative Custom Dictionary is *PrivacyDIC*.

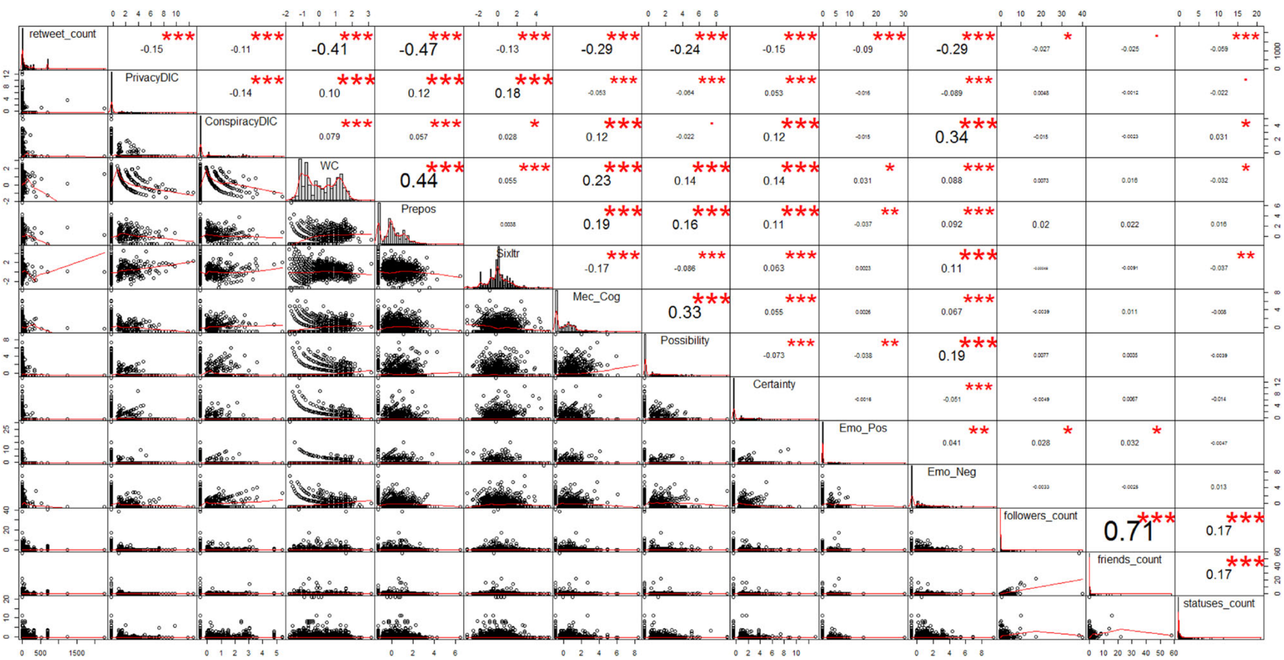


FIGURE 3 Variables inter-correlations, pairwise scatterplots and histograms

The model on *privacy* correctly classifies 89.4% of tweets, with the most important predictor represented by our category *PrivacyDIC* (Table 3). Noteworthy, the relative influence of *PrivacyDIC* is almost five times the second category, showing that the words that Twitter users use to communicate their *privacy concerns* are clearer than other characteristics of the text posted on the social media.

The model on *conspiracy* provides a different picture. The AI machine correctly classifies 68.3% of tweets, with the most important predictor represented by our category *ConspiracyDIC* (Table 3). Our custom dictionary displays a relative influence weaker than in the *privacy* analysis. In fact, in this case, Twitter users cast their contents by mixing words that are specific to conspiracy theories through a more articulate style with longer and more complex tweets including prepositions, cognitive mechanisms and negative emotions.

Overall, these results suggest that *privacy concerns* are sharper compared to *conspiracy theories*. Thus, detecting tweets containing *privacy concerns* is easier than *conspiracy theories*. Results also support that the two domains are reflected by different uses of textual elements. In fact, *ConspiracyDIC* is marginal in detecting *privacy concerns* and *PrivacyDIC* is marginal in detecting *conspiracy theories*.

3.2 | Study 2

Building on the results of the previous analyses, we estimated a Poisson model on the retweet count of the 5615 tweets. We used the number of retweets as the dependent variable, *PrivacyDIC*, *ConspiracyDIC* and *text complexity*, *certainty in language* and *emotions* as independent variables. We also added the Twitter users' characteristics and the presence of media elements as controls. To test hypotheses H1-H5 we calculated the full Model 8. Models 1-7 provide partial model estimates. In particular, we first calculated the intercept model, taken as a base model for further comparisons (Model 1). Then, we calculated Model 2 using *PrivacyDIC* (H1) and *ConspiracyDIC* (H2), Model 3 using *text complexity* (H3), Model 4 using *certainty in language* (H4) and Model 5 using *emotions* (H5). Model 6 includes all hypotheses-related variables and finally, Model 7 includes only the control variables. Inter-correlations between variables, pairwise scatterplots and histograms are depicted in Figure 3.

Table 4 below reports the results of our Poisson analysis using standardized variables. The differences between the full model and all the sub-models are significant ($P(\chi^2$, df)<1e-03).

The intercepts are significant and positive in all models, suggesting a baseline effect of the keywords used to sample the tweets, irrespective of the characteristics of the text and control variables.

In Model 8, *PrivacyDIC* is significant and negative (−0.222, p(>|z|)<2e-16), indicating that the inclusion of *privacy concerns* in the text may inhibit the diffusion of the tweet, providing an interesting and counterintuitive effect against our expectations of hypothesis H1. Meanwhile, *ConspiracyDic* is significant and positive (0.215, p(>|z|)<2e-16), indicating that the inclusion of *conspiracy theories* appeals to users, supporting H2. This pattern is consistent with the picture provided by Model 6, i.e. the model without control variables. These results, together with the evidence of the preliminary analyses, suggest that the communication of *privacy concerns* is more explicit than the inclusion of *conspiracy theories*, cueing different readers' reactions that translate into a different likelihood of retweeting the tweet.

Model 8 fully supports hypothesis H3. Results on *text complexity* (*word count:* −0.100, p(>|z|)<2e-16; *prepositions:* −0.568, p(>|z|)<2e-16; *six letters:* −0.304, p(>|z|)<2e-16; *cognitive mechanism* −0.416, p(>|z|)<2e-16) can be interpreted more easily considering the results reported in Table 3. Specifically, in the case of *conspiracy theories*, the complexity of a tweet has a higher relative influence than in the case of tweets characterized by *privacy concerns*. These results converge in indicating that high *text complexity* requires a supplement of the reader's attention, inhibiting the retweet.

Contrary to our expectations for hypothesis H4a, data provide a counterintuitive negative direction of the effect of *certainty* in language (−0.280, p(>|z|)<2e-16). Meanwhile, H4b is supported (−0.516, p(>|z|)<2e-16), indicating that tentative language inhibits the diffusion of a tweet. This pattern suggests that a text including *privacy concerns* and/or *conspiracy theories* stimulates retweets when the language used is sneaky and doubtful. On the one hand, this interpretation is consistent to a general trend of including jokes, memes, icons, trolling and sarcasm in tweets. On the other hand, our results support that the high uncertainty of people in facing the COVID-19 pandemic (and related issues) translates in a diffused debate fed by tentative speculations and theories.

Contrary to our expectations for hypotheses H5a-b, data supports significant and negative effects of both *positive* (−0.530, p(>|z|)<2e-16) and *negative* (−0.331, p(>|z|)<2e-16) emotions. Therefore, Twitter users are likely appealed by COVID-related propositions presented without emotional emphasis, as well as without certainty in language (as suggested by results on hypothesis H4).

Finally, based on the likelihood ratios, the improvement of Model 7 on Model 1 is weaker than the improvement of Model 6 and the full Model 8, indicating that the contribution of the control variables in explaining the variance of the dependent variables is marginal. Thus, these estimates suggest that the Twitter users actually read the tweets before retweeting (even though our results do not offer any insight about whether they understand the tweets) and their behavior is only marginally cued by the status of the author or the inclusion of media.

In Figure 4 we visually summarize our results.

4 | DISCUSSION AND CONCLUSIONS

This paper aims to explore which words, linguistic style, and emotions conveyed by tweets are more likely to be associated with *privacy concerns* and *conspiracy theories* and how they affect virality. By developing two custom dictionaries related to *privacy concerns* and *conspiracy theories* and by analyzing which type of language is more likely to affect tweets' virality, we found support to our research proposition.

Our results suggest that words associated with *privacy concerns* and *conspiracy theories* belong to two different domains. Overall, *conspiracy theories* improve the probability of retweeting a text but, contrary to our expectations, *privacy concerns* inhibit the virality of a tweet. Noteworthy, the complexity of the language used negatively affects retweets suggesting that tweets are more effective when they use simple texts, thus avoiding high cognitive loads for the reader. Data also provides an intriguing picture of the effects of emotions and certainty in language. In fact, consistent with Aleti et al. (2019), we found that emotions in text may inhibit retweets while, contrary to Pezzuti et al. (2021), we found that also certainty in language reduces users' engagement (i.e., retweets). This pattern of results adds to the scholarly debate, and it is consistent with the high uncertainty that characterizes the Twitter debate on the usage of a contact-tracing app to stem the COVID-19 pandemic.

These results contribute to the literature in different ways. First, we contribute to the growing body of literature that builds on the intersection between psychology, marketing and linguistics (e.g., Aleti et al., 2019; Berger et al., 2020; Netzer et al., 2019; Packard & Berger, 2019; Labrecque et al., 2020). This stream of literature suggests that a text reflects and indicates something about its author and impacts the audience (e.g., Berman et al., 2019; Cruz et al., 2017; Labrecque et al., 2020; Massara et al., 2020; Van Laer et al., 2019). However, this academic debate overlooks the role of *privacy concerns* and *conspiracy theories*, so far. The relevance of these topics surpasses the boundaries of the social media realm and translates into real threats for companies. The present paper contributes to shedding light on the detectability of *privacy*

TABLE 4 Models (independent variable standardized)

	Model 1	Model 2	Model 3	Model 4	Model 5	Model 6	Model 7	Model 8
H1-2: Tweets' topic								
PrivacyDIC		−0.659***				−0.277***		−0.222***
		(0.003)				(0.003)		(0.003)
ConspiracyDIC		−0.283***				0.177***		0.215***
		(0.002)				(0.001)		(0.002)
H3: Text complexity								
Wordcount			−0.255***			0.004**		−0.100***
			(0.002)			(0.002)		(0.002)
Prepositions			−0.750***			−0.712***		−0.568***
			(0.002)			(0.002)		(0.002)
Six letters			−0.346***			−0.296***		−0.304***
			(0.001)			(0.001)		(0.001)
Cognitive mechanisms			−0.400***			−0.359***		−0.416***
			(0.002)			(0.002)		(0.002)
H4: Certainty vs tentative								
Tentative				−1.039***		−0.488***		−0.516***
				(0.003)		(0.003)		(0.003)
Certainty				−0.502***		−0.245***		−0.280***
				(0.002)		(0.002)		(0.002)
H5: Emotions								
Positive emotions					−0.523***	−0.540***		−0.530***
					(0.005)	(0.005)		(0.005)
Negative emotions					−0.934***	−0.525***		−0.331***
					(0.002)	(0.002)		(0.002)
Control variables								
Followers Count							0.019***	0.005***
							(0.001)	(0.001)
Friends Count							−0.083***	−0.017***
							(0.003)	(0.002)
Statuses Count							−0.132***	−0.063***
							(0.002)	(0.002)
url:yes							−2.212***	−2.082***
							(0.008)	(0.008)
media:photo							−2.605***	−2.555***
							(0.023)	(0.023)
Intercept	4.897***	4.764***	4.342***	4.550***	4.561***	4.081***	5.099***	4.359***
	(0.001)	(0.001)	(0.002)	(0.002)	(0.002)	(0.002)	(0.001)	(0.002)
Log Likelihood	−821,594.4	−759,481.1	−460,717.4	−676,967.6	−673,618.1	−362,345.7	−700,952.7	−270,540.0

Note: *$p < .1$; **$p < 0.05$; ***$p < 0.01$.

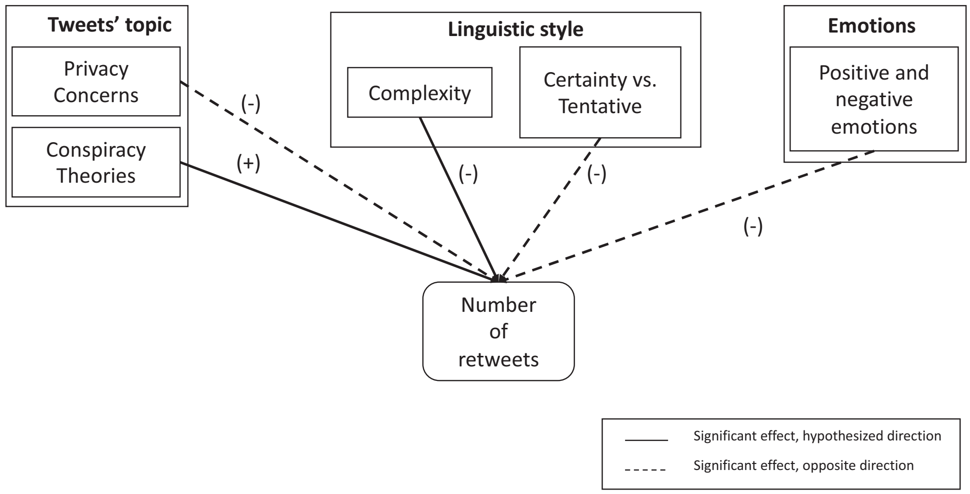


FIGURE 4 Summary of results

concerns and *conspiracy theories* and on their power to feed virality before translating words into action.

Second, one of the reasons behind the lack of studies analysing privacy concerns and conspiracy theories as topics of discussion on social media platforms may be the absence of tools for measuring them in natural language. Our crafted dictionaries will thus represent a valuable starting point for future research delving deep into the analysis of how consumers express privacy concerns and conspiracy theories in digital environments.

Third, while most research tends to focus on either prediction or understanding of different types of texts (Berger et al., 2020), in this paper we integrate both aspects by illustrating how tweets are composed in terms of privacy and conspiracy topics as well as how these features predict the virality of the tweets. Indeed, we develop and test ad hoc dictionaries to detect *privacy concerns* and *conspiracy theories* in social media textual contents without the inclusion of any direct link to the Italian governmental tracing app (namely, Immuni) used as empirical context. This provides an approach that can be generalized to the detection of social media users' attitudes towards apps and platforms that exploit user data to market their services. Furthermore, since language expresses a concept through a *pattern* of symbols (namely: words), we introduced the possibilities provided by *machine learning* algorithms to stimulate the debate in our disciplines. In fact, as far as we know, the validation process is usually made only thanks to external human coders. Differently, in our paper, we also applied machine learning techniques to actually assess the predictive power of our dictionaries, as this approach is widely used in *pattern matching* (e.g., Lemmens & Croux, 2006; Lemmens & Gupta, 2020).

Fourth, our results are of relevance for the marketing discipline since they provide empirical evidence on how users react to technologies that might be associated with consumers' *privacy concerns* (Plangger & Montecchi, 2020). Data indeed supports the need for continuous social media listening to detect the possible spread of massive negative word-of-mouth related to *privacy concerns* or *conspiracy theories*.

This study provides also several managerial implications. First, the adoption of the two custom dictionaries could be a valuable support in identifying the main psychological barriers to the adoption of apps and platforms including contact-tracing apps. Second, by identifying the characteristics that drive tweets virality, we provide indications to marketers about how to engage with social media users and eventually limit the spread of misinformation about social initiatives in the internet realm. As Twitter is increasingly recognised as an important medium to reach consumers (Berman et al., 2019), marketers and policy-makers could benefit from the results of this study to have a deeper understanding of their customers and plan specific strategies to cope with the spreading of (disproportional) privacy concerns and conspiracy theories, while constantly monitoring the information flowing through the platform. Third, far from suggesting any form of censorship on social media, we find that *privacy concerns* are clearly identifiable by monitoring a reduced set of keywords.

In line with the literature on fake news (Cova & D'Antone, 2016; Di Domenico & Visentin, 2020), we suggest that brand managers can turn a threat originated from brand-related *privacy concerns* or *conspiracy theories* into an opportunity, namely an enrichment of the set of brand associations.

Finally, we must acknowledge that our results can be used both to better respond to the needs of people and businesses and to be more effective in acting harmfully. However, this is a general warning about all marketing tools—as the AMS statement of ethics requires explicitly to use marketing avoiding harmful actions (https://www.ama.org/codes-of-conduct/). Furthermore, if a bad actor would use our results to run a troll farm, we believe that it would be easily identified and stopped just by using our findings against it.

4.1 | Limitations and future research

To fully appreciate the theoretical and managerial contributions of our results, we acknowledge some limitations affecting our study. First, both the *privacyDIC* and *conspiracyDIC* dictionaries are built in the Italian language. This might limit their applicability to other international social media contexts. However, since texts are shaped by the cultural context in which they are produced (e.g., Berger et al., 2020; Cruz et al., 2017) we suggest using our methodology to develop language-specific dictionaries.

Second, our study focuses on the analysis of the spreading of *privacy concerns* and *conspiracy theories* on Twitter. It would be interesting analysing how these contents spread through other social media platforms and if there are other contents' or platform-specific characteristics.

Third, in this study, we focus on *privacy concerns* as a barrier to the adoption of contact-tracing apps without evaluating its impact on the actual adoption rates of said digital surveillance technologies. Thus, further research should assess the extent to which *privacy concerns* (and *conspiracy theories*) can limit the actual consumers' behavioural intentions to adopt contact-tracing apps.

Finally, we acknowledge that users' concerns about privacy seem to be somewhat disproportionate as governmental contact-tracing apps are actually much less privacy-invasive than other widely used social media apps. This effect could be explained in terms of the utilitarian versus hedonic use of apps (Scarpi, 2021). Even though we did not address explicitly this point in our study, we think that individuals' over warning deserves further research.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ORCID

Marco Visentin http://orcid.org/0000-0003-2943-6484
Annamaria Tuan http://orcid.org/0000-0003-1471-3063
Giandomenico Di Domenico http://orcid.org/0000-0002-5420-8750

REFERENCES

Agosti, A., & Rellini, A. (2007). *The Italian LIWC Dictionary*. LIWC.net.

Ahmed, W., Vidal-Alaball, J., Downing, J., & Seguí, F. L. (2020). COVID-19 and the 5G conspiracy theory: social network analysis of Twitter data. *Journal of Medical Internet Research*, *22*(5), e19458.

Akpinar, E., & Berger, J. (2017). Valuable virality. *Journal of Marketing Research*, *54*(2), 318–330.

Aleti, T., Pallant, J. I., Tuan, A., & van Laer, T. (2019). Tweeting with the stars: Automated text analysis of the effect of celebrity social media communications on consumer word of mouth. *Journal of Interactive Marketing*, *48*, 17–32.

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of economic perspectives*, *31*(2), 211–236.

Amann, J., Sleigh, J., & Vayena, E. (2021). Digital contact-tracing during the Covid-19 pandemic: An analysis of newspaper coverage in Germany, Austria, and Switzerland. *PLoS One*, *16*(2), e0246524.

Appel, G., Grewal, L., Hadi, R., & Stephen, A. T. (2020). The future of social media in marketing. *Journal of the Academy of Marketing Science*, *48*(1), 79–95.

Appleby, J. (2020). Conspiracy theories aside, here's what contact tracers really do. https://californiahealthline.org/news/conspiracy-theoriesaside-heres-what-contact-tracers-really-do/

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26–53.

Bazarova, N. N., & Masur, P. K. (2020). Towards an integration of individualistic, networked, and institutional approaches to online disclosure and privacy in a networked ecology. *Current Opinion in Psychology*, *36*, 118–123.

Berger, J., Humphreys, A., Ludwig, S., Moe, W. W., Netzer, O., & Schweidel, D. A. (2020). Uniting the tribes: Using text for marketing insight. *Journal of Marketing*, *84*(1), 1–25.

Berger, J., & Milkman, K. L. (2012). What makes online content viral? *Journal of Marketing Research*, *49*(2), 192–205.

Berman, R., Melumad, S., Humphrey, C., & Meyer, R. (2019). A tale of two Twitterspheres: Political microblogging during and after the 2016 primary and presidential debates. *Journal of Marketing Research*, *56*(6), 895–917.

Bertele, K., Feiereisen, S., Storey, C., & van Laer, T. (2020). It's not what you say, it's the way you say it! Effective message styles for promoting innovative new services. *Journal of Business Research*, *107*, 38–49.

Billett, M. T., Jiang, Z., & Rego, L. L. (2014). Glamour brand and glamour stocks. *Journal of Economic Behavior and Organization*, *107*, 744–759.

Birnbaum, M., & Spolar, C. (2020). Coronavirus tracking apps meet resistance in privacy-conscious Europe. *The Washington Post*.

Blose, T., Umar, P., Squicciarini, A., & Rajtmajer, S. (2020). Privacy in Crisis: A study of self-disclosure during the Coronavirus pandemic. *arXiv preprint arXiv:2004.09717*.

Bost, P. R., & Prunier, S. G. (2013). Rationality in conspiracy beliefs: The role of perceived motive. *Psychological Reports*, *113*(1), 118–128.

Bright, L. F., Lim, H. S., & Logan, K. (2021). "Should I Post or Ghost?": Examining how privacy concerns impact social media engagement in US consumers. *Psychology & Marketing*, 1–11. online first.

Bryan, A. D., Webster, G. D., & Mahaffey, A. L. (2011). The big, the rich, and the powerful: Physical, financial, and social dimensions of dominance in mating and attraction. *Personality and Social Psychology Bulletin*, *37-3*, 365–382.

Byford, J. (2011). *Conspiracy theories: A critical introduction*. Springer.

Cambridge (2020). *Certainty Meaning In The Cambridge English Dictionary*. [online] Dictionary.cambridge.org. Available at: https://dictionary.cambridge.org/it/dizionario/inglese/certainty. Accessed October 23, 2020.

Chang, Y. K., Hung, C. L., Timme, S., Nosrat, S., & Chu, C. H. (2020). Exercise behavior and mood during the COVID-19 pandemic in Taiwan: Lessons for the future. *International Journal of Environmental Research and Public Health*, *17*(19), 7092.

Chen, H. T., & Kim, Y. (2013). Problematic use of social network sites: The interactive relationship between gratifications sought and privacy concerns. *Cyberpsychology, Behavior and Social Networking*, *16*(11), 806–812.

Chen, R., & Sakamoto, Y. (2014, January). Feelings and perspective matter: Sharing of crisis information in social media. In *2014 47th Hawaii International Conference on System Sciences* (pp. 1958-1967). IEEE.

Choi, T. R., & Sung, Y. (2018). Instagram versus Snapchat: Self-expression and privacy concern on social media. *Telematics and informatics*, *35*(8), 2289–2298.

Chou, W. Y. S., Oh, A., & Klein, W. M. (2018). Addressing health-related misinformation on social media. *Journal of the American Medical Association*, *320*(23), 2417–2418.

Colleoni, E., Rozza, A., & Arvidsson, A. (2014). Echo chamber or public sphere? Predicting political orientation and measuring political homophily in Twitter using big data. *Journal of Communication*, *64*(2), 317–332.

Corbin, J., & Strauss, A. (2014). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications

Cova, B., & D'Antone, S. (2016). Brand iconicity vs. anti-consumption well-being concerns: The Nutella palm oil conflict. *Journal of Consumer Affairs*, *50*(1), 166–192.

Cruz, R. E., Leonhardt, J. M., & Pezzuti, T. (2017). Second person pronouns enhance consumer involvement and brand attitude. *Journal of Interactive Marketing*, *39*, 104–116.

Cuan-Baltazar, J. Y., Muñoz-Perez, M. J., Robledo-Vega, C., Pérez-Zepeda, M. F., & Soto-Vega, E. (2020). Misinformation of COVID-19 on the internet: infodemiology study. *JMIR Public Health and Surveillance*, *6*(2), e18444.

De Vries, L., Gensler, S., & Leeflang, P. S. (2012). Popularity of brand posts on brand fan pages: An investigation of the effects of social media marketing. *Journal of interactive marketing*, *26*(2), 83–91.

Degirmenci, K. (2020). Mobile users' information privacy concerns and the role of app permission requests. *International Journal of Information Management*, *50*, 261–272.

Del Vicario, M., Bessi, A., Zollo, F., Petroni, F., Scala, A., Caldarelli, G., Stanley, H. E., & Quattrociocchi, W. (2016). The spreading of misinformation online. *Proceedings of the National Academy of Sciences*, *113*(3), 554–559.

Di Domenico, G., & Visentin, M. (2020). Fake news or true lies? Reflections about problematic contents in marketing. *International Journal of Market Research*, *62*(4), 409–417.

Di Domenico, G., Sit, J., Ishizaka, A., & Nunan, D. (2021). Fake news, social media and marketing: A systematic review. *Journal of Business Research*, *124*, 329–341.

Dienlin, T., Masur, P. K., & Trepte, S. (2019). A longitudinal analysis of the privacy paradox. *New Media & Society*, 14614448211016316.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285–297.

Douglas, K. M., Sutton, R. M., & Cichocka, A. (2017). The psychology of conspiracy theories. *Current directions in psychological science*, *26*(6), 538–542.

Fisher, M. (2020). Why coronavirus conspiracy theories flourish. and why it matters. *The New York Times*, *8*.

Friedman, J., Hastie, T., & Tibshirani, R. (2000). Additive logistic regression: a statistical view of boosting (with discussion and a rejoinder by the authors). *The annals of statistics*, *28*(2), 337–407.

Friedman, J. H. (2002). Stochastic gradient boosting. *Computational statistics & data analysis*, *38*(4), 367–378.

Georgiou, N., Delfabbro, P., & Balzan, R. (2020). COVID-19-related conspiracy beliefs and their relationship with perceived stress and pre-existing conspiracy beliefs. *Personality and Individual Differences*, *166*, 110201.

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security*, *77*, 226–261.

Gruzd, A., & Mai, P. (2020). Going viral: How a single tweet spawned a COVID-19 conspiracy theory on Twitter. *Big Data & Society*, *7*(2), 2053951720938405.

Gu, J., Xu, Y. C., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*, *94*, 19–28.

Hansen, L. K., Arvidsson, A., Nielsen, F. Å., Colleoni, E., & Etter, M. (2011). Good friends, bad news-affect and virality in twitter, *Future information technology* (pp. 34–43). Springer.

Harris, M. A., Brookshire, R., & Chin, A. G. (2016). Identifying factors influencing consumers' intent to install mobile applications. *International Journal of Information Management*, *36*(3), 441–450.

Hart, R. P., & Childers, J. P. (2004). Verbal certainty in American politics: An overview and extension. *Presidential Studies Quarterly*, *34*(3), 516–535.

Hart, W., Albarracín, D., Eagly, A. H., Brechan, I., Lindberg, M. J., & Merrill, L. (2009). Feeling validated versus being correct: a meta-analysis of selective exposure to information. *Psychological Bulletin*, *135*(4), 555–588.

Herhausen, D., Ludwig, S., Grewal, D., Wulf, J., & Schoegel, M. (2019). Detecting, preventing, and mitigating online firestorms in brand communities. *Journal of Marketing*, *83*(3), 1–21.

Hewett, K., Rand, W., Rust, R. T., & Van Heerde, H. J. (2016). Brand buzz in the echoverse. *Journal of Marketing*, *80*(3), 1–24.

Hinds, J., Williams, E. J., & Joinson, A. N. (2020). "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies*, *143*, 102498.

Hirsh, J. B., & Peterson, J. B. (2009). Personality and language use in self-narratives. *Journal of Research in Personality*, *43*(3), 524–527.

Hollebeek, L. D., & Macky, K. (2019). Digital content marketing's role in fostering consumer engagement, trust, and value: Framework, fundamental propositions, and implications. *Journal of Interactive Marketing*, *45*, 27–41.

Humphreys, A., & Wang, R. J. H. (2018). Automated text analysis for consumer research. *Journal of Consumer Research*, *44*(6), 1274–1306.

Jeong, Y., & Kim, Y. (2017). Privacy concerns on social networking sites: Interplay among posting types, content, and audiences. *Computers in Human Behavior*, *69*, 302–310.

Kearney, M. D., Chiang, S. C., & Massey, P. M. (2020). The Twitter origins and evolution of the COVID-19 "plandemic" conspiracy theory. *Harvard Kennedy School Misinformation Review*, *1*(3).

Keib, K., Himelboim, I., & Han, J. Y. (2018). Important tweets matter: Predicting retweets in the# BlackLivesMatter talk on twitter. *Computers in Human Behavior*, *85*, 106–115.

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.

Klein, C., Clutton, P., & Dunn, A. G. (2019). Pathways to conspiracy: The social and linguistic precursors of involvement in Reddit's conspiracy theory forum. *PLoS One*, *14*(11), e0225098.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, *64*, 122–134.

Labrecque, L. I., Swani, K., & Stephen, A. T. (2020). The impact of pronoun choices on consumer engagement actions: Exploring top global brands' social media communications. *Psychology & Marketing*, *37*(6), 796–814.

Lamberton, C., & Stephen, A. T. (2016). A thematic exploration of digital, social media, and mobile marketing: Research evolution from 2000 to 2015 and an agenda for future inquiry. *Journal of Marketing*, *80*(6), 146–172.

Lee, D., Hosanagar, K., & Nair, H. S. (2018). Advertising content and consumer engagement on social media: evidence from Facebook. *Management Science*, *64*(11), 5105–5131.

Leek, S., Houghton, D., & Canning, L. (2019). Twitter and behavioral engagement in the healthcare sector: An examination of product and service companies. *Industrial Marketing Management*, *81*, 115–129.

Lemmens, A., & Croux, C. (2006). Bagging and boosting classification trees to predict churn. *Journal of Marketing Research*, *43*(2), 276–286.

Lemmens, A., & Gupta, S. (2020). Managing churn to maximize profits. *Marketing Science*, *39*(5), 956–973.

Love, B. (2020). *Covid tracing fans public health vs privacy debate*. The Financial Times.

Ludwig, S., De Ruyter, K., Friedman, M., Brüggen, E. C., Wetzels, M., & Pfann, G. (2013). More than words: The influence of affective content and linguistic style matches in online reviews on conversion rates. *Journal of Marketing*, *77*(1), 87–103.

Maseeh, H. I., Jebarajakirthy, C., Pentecost, R., Arli, D., Weaven, S., & Ashaduzzaman, M. (2021). Privacy concerns in e-commerce: A multilevel meta-analysis. *Psychology & Marketing*, 1–20.

Mashuri, A., & Zaduqisti, E. (2014). The role of social identification, intergroup threat, and out-group derogation in explaining belief in conspiracy theory about terrorism in Indonesia. *International Journal of Research Studies in Psychology*, *3*(1), 35–50.

Massara, F., Scarpi, D., & Porcheddu, D. (2020). Can Your Advertisement Go Abstract Without Affecting Willingness to Pay?: Product-Centered versus Lifestyle Content In Luxury Brand Print Advertisements. *Journal of Advertising Research*, *60*(1), 28–37.

McAdams, D. P. (2001). The psychology of life stories. *Review of general psychology*, *5*(2), 100–122.

McGinty, M., & Gyenes, N. (2020). A dangerous misinfodemic spreads alongside the SARS-COV-2 pandemic. *Harvard Kennedy School Misinformation Review*, *1*(3).

Miller, J., & Abboud, L. (2020). German u-turn over coronavirus tracking app sparks backlash. *The Financial Times*

Morse, J. M., Olson, K., & Spiers, J. (2002). Verification strategies for establishing reliability and validity in qualitative research. *International Journal of Qualitative Methods*, *1*(2), 13–22.

Natekin, A., & Knoll, A. (2013). Gradient boosting machines, a tutorial. *Frontiers in Neurorobotics*, *7*, 21.

Netzer, O., Lemaire, A., & Herzenstein, M. (2019). When words sweat: Identifying signals for loan default in the text of loan applications. *Journal of Marketing Research*, *56*(6), 960–980.

Nikolinakou, A., & King, K. W. (2018). Viral video ads: Emotional triggers and social media virality. *Psychology & Marketing*, *35*(10), 715–726.

Osatuyi, B. (2015). Is lurking an anxiety-masking strategy on social media sites? The effects of lurking and computer anxiety on explaining information privacy concern on social media platforms. *Computers in Human Behavior*, *49*, 324–332.

Packard, G., & Berger, J. (2019). How Concrete Language Shapes Customer Satisfaction. *ACR North American Advances*

Pedersen, C. L. (2021). Empathy-based marketing. *Psychology & Marketing*, *38*(3), 470–480.

Pennebaker, J. W., Booth, R. J., & Francis, M. E. (2007). Operator's manual: Linguistic inquiry and word count: LIWC2007. *Austin, Texas: LIWC. net* http://homepage.psy.utexas.edu/HomePage/Faculty/Pennebaker/Reprints/LIWC2007_OperatorManual.pdf. Accessed September 1, 2020.

Pennebaker, J. W., Mehl, M. R., & Niederhoffer, K. G. (2003). Psychological aspects of natural language use: Our words, our selves. *Annual Review of Psychology*, *54*(1), 547–577.

Peters, K., Chen, Y., Kaplan, A. M., Ognibeni, B., & Pauwels, K. (2013). Social media metrics—A framework and guidelines for managing social media. *Journal of Interactive marketing*, *27*(4), 281–298.

Pezzuti, T., Leonhardt, J. M., & Warren, C. (2021). Certainty in Language Increases Consumer Engagement on Social Media. *Journal of Interactive Marketing*, *53*, 32–46.

Pizzi, G., & Scarpi, D. (2020). Privacy threats with retail technologies: A consumer perspective. *Journal of Retailing and Consumer Services*, *56*, 102160.

Plangger, K., & Montecchi, M. (2020). Thinking Beyond Privacy Calculus: Investigating Reactions to Customer Surveillance. *Journal of Interactive Marketing*, *50*, 32–44.

Quattrociocchi, W., Scala, A., & Sunstein, C. R. (2016). Echo chambers on Facebook. *Available at SSRN 2795110*.

Rehman, Z. U., Baharun, R., & Salleh, N. Z. M. (2020). Antecedents, consequences, and reducers of perceived risk in social media: A systematic literature review and directions for further research. *Psychology & Marketing*, *37*(1), 74–86.

Ridgeway, G., & Ridgeway, M. G. (2004). The gbm package. *R Foundation for Statistical Computing, Vienna, Austria*, *5*(3).

Rimé, B. (2009). Emotion elicits the social sharing of emotion: Theory and empirical review. *Emotion review*, *1*(1), 60–85.

Rudat, A., Buder, J., & Hesse, F. W. (2014). Audience design in Twitter: Retweeting behavior between informational value and followers' interests. *Computers in Human Behavior*, *35*, 132–139.

Rust, R. T., Rand, W., Huang, M. H., Stephen, A. T., Brooks, G., & Chabuk, T. (2021). Real-time brand reputation tracking using social media. *Journal of Marketing*, 0022242921995173.

Scarpi, D. (2021). A construal-level approach to hedonic and utilitarian shopping orientation. *Marketing Letters*, *32*(2), 261–271.

Shibchurn, J., & Yan, X. (2015). Information disclosure on social networking sites: An intrinsic–extrinsic motivation perspective. *Computers in Human Behavior*, *44*, 103–117.

Shilton, K., & Greene, D. (2019). Linking platforms, practices, and developer ethics: Levers for privacy discourse in mobile application development. *Journal of Business Ethics*, *155*(1), 131–146.

Shin, W., & Kang, H. (2016). Adolescents' privacy concerns and information disclosure online: The role of parents and the Internet. *Computers in Human Behavior*, *54*, 114–123.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, *35*, 989–1015.

Sweeney, Y. (2020). Tracking the debate on COVID-19 surveillance tools. *Nature Machine Intelligence*, *2*, 301–304.

Tausczik, Y. R., & Pennebaker, J. W. (2010). The psychological meaning of words: LIWC and computerized text analysis methods. *Journal of language and social psychology*, *29*(1), 24–54.

Tellis, G. J., MacInnis, D. J., Tirunillai, S., & Zhang, Y. (2019). What drives virality (sharing) of online digital content? The critical role of information, emotion, and brand prominence. *Journal of Marketing*, *83*(4), 1–20.

Tetlock, P. E. (2002). Social functionalist frameworks for judgment and choice: intuitive politicians, theologians, and prosecutors. *Psychological Review*, *109*(3), 451–471.

Trang, S., Trenz, M., Weiger, W. H., Tarafdar, M., & Cheung, C. M. (2020). One app to trace them all? Examining app specifications for mass acceptance of contact-tracing apps. *European Journal of Information Systems*, *29*, 1–14.

Vanhaecht, K., Seys, D., Bruyneel, L., Cox, B., Kaesemans, G., Cloet, M., & Claes, S. (2020). COVID-19 is having a destructive impact on health-care workers' mental well-being. *International Journal for Quality in Health Care*

Van Laer, T., Edson Escalas, J., Ludwig, S., & Van Den Hende, E. A. (2019). What happens in Vegas stays on TripAdvisor? A theory and technique to understand narrativity in consumer reviews. *Journal of Consumer Research*, *46*(2), 267–285.

Van Prooijen, J. W. (2018). *The psychology of conspiracy theories*. Routledge.

Van Prooijen, J. W., & Jostmann, N. B. (2013). Belief in conspiracy theories: The influence of uncertainty and perceived morality. *European Journal of Social Psychology*, *43*(1), 109–115.

Vicario, M. D., Quattrociocchi, W., Scala, A., & Zollo, F. (2019). Polarization and fake news: Early warning of potential misinformation targets. *ACM Transactions on the Web (TWEB)*, *13*(2), 1–22.

Villarroel Ordenes, F., Ludwig, S., De Ruyter, K., Grewal, D., & Wetzels, M. (2017). Unveiling what is written in the stars: Analyzing explicit, implicit, and discourse patterns of sentiment in social media. *Journal of Consumer Research*, *43*(6), 875–894.

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, *359*(6380), 1146–1151.

Wood, M. J. (2018). Propagating and debunking conspiracy theories on Twitter during the 2015–2016 Zika virus outbreak. *Cyberpsychology, Behavior and Social Networking*, *21*(8), 485–490.

Xu, W. W., & Zhang, C. (2018). Sentiment, richness, authority, and relevance model of information sharing during social Crises—the case of# MH370 tweets. *Computers in Human Behavior*, *89*, 199–206.

Zhao, L., Lu, Y., & Gupta, S. (2012). Disclosure intention of location-related information in location-based social network services. *International Journal of Electronic Commerce*, *16*(4), 53–90.

How to cite this article: Visentin, M., Tuan, A., & Di Domenico, G. (2021). Words matter: How privacy concerns and conspiracy theories spread on Twitter. *Psychol Mark*, 38, 1828–1846. https://doi.org/10.1002/mar.21542

APPENDIX A

CONSPIRACY

"Conspiracy theories" are attempts to explain the ultimate causes of significant social and political events and circumstances with claims of secret plots by two or more powerful actors. Conspiracy beliefs have the potential to cause harm both to the individual and the community. Conspiracy endorsement is associated with lowered intention to participate in social and political causes, unwillingness to follow authoritative medical advice, increased willingness to seek alternative medicine, and a tendency to reject important scientific findings.

Consistent to this definition of ***conspiracy theory***, **please put 1 if, in your opinion, each word in the sheet "conspiracy" fits in the category and 0 otherwise.**

PRIVACY CONCERNS

Privacy concern has become an important ethical issue of the information age. Privacy may be a concern when people are aware that information about them is being collected without their permission and/or they do not know specifically how the information is being used. In the context of online marketing, privacy concern refers to the degree to which an Internet user is concerned about online marketers' collection, dissemination, and use of his/her personal information.

Consistent to this definition of ***privacy concern***, **please put 1 if, in your opinion, each word in the sheet "privacy" fits in the category and 0 otherwise.**

BOTH

In some cases conspiracy and privacy issues are interrelated. In the third sheet you will find a list of words related to both topics. please rate the extent to which each word is related to the category "both" as a mix between conspiracy and privacy.

Please put 1 if, in your opinion, each word in the sheet "both" fits in the category and 0 otherwise.

It would be great if you can help us in developing the dictionary. If you think that some additional words are needed, please suggest them to us.

APPENDIX B: DICTIONARIES *PRIVACYDIC* AND *CONSPIRACYDIC*

PrivacyDIC		*ConspiracyDIC*	
Italian	**English**	**Italian**	**English**
anonimo	anonymous	aerei dirottati	Hijacked planes
Blocca*	Block*	annienta*	Annihilat*
Codice sorgente	Source code	campagna di terrore	Terror campaign
consens*	consent	Colpa	Blame
Contact tracing	Contact Tracing	Complott*	Plot*
cybersecurity	cybersecurity	Conservazione dei poteri	Power preservation
Dati	Data	Cospirazionismo	Conspiracy theories
garan*	guarantee	Criminal*	Criminal*
Geolocalizzazion*	Geolocation	Delinquent*	Delinquent*
GPS	GPS	distruggeremo	Destroy
Grande fratello	Big brother	dittator*	Dictator*
pin	pin	Dittatur*	Dictatorship
policy	policy	Dominare	Dominate
posizion*	position	doppiogiochismo	Double-dealing
Privacy	Privacy	emergenza mentale	Mental emergency
Profila	Profiling	controll*	Control*
profilaz*	Profiling	Gente	People
proteggere	Protect	Governo	Government
protezion*	Protection*	governodincapaci	Government of incompetents
registr*	Register/registration	incapaci	Incompetents
Schedat*	File*	invadono	Invade
senza permesso	Without consent	ipocrisia	Hypocrisy

(Continues)

PrivacyDIC		*ConspiracyDIC*	
Italian	**English**	**Italian**	**English**
Sicurezz*	Security	Mafi*	Maphia*
Social media	Social media	manipolano	Manipulate
social	social	Meccanismo	Mechanism
Sorveglianza	Surveillance	mentite	Lie
Spia*	Spy*	Mi spiegate	Explain to me
Traccia*	Track*	Negazionist*	Denialist*
Tracing	Tracing	Noallamuseruola	No to the muzzle
Tutel*	Protect*	Omertà	Omerta/conspiracy of silence
Violat*	Violat*	Padroni	Lords
		Poter*	Power*
		Propagand*	Propaganda
		Regim*	Regimen*
		Rifilarci	Foist on us
		Riprenderemo	Take back
		ruba	Steal*
		Sanno	Know
		Sapeva	He/she knew
		Se ne fregano	They don't care
		servitù	Servitude
		social credit system	Social credit system
		Soldi	Money
		sopressione	Suppression
		squola	School
		Stato	Country/state
		stato di emergenza	State of emergency
		Subdola	Subtle
		Suddit*	Servant*
		Terror*	Terror*
		Truffa	Fraud
		Usurpator*	Usurp*
		Vi vogliono	They want you to
		virus artificiali	Artificial viruses

Note: the translation is provided for readers' convenience. Non-Italian scholars and practitionners should develop their language-specific *PrivacyDIC* and *ConspiracyDIC* following the methodology herein presented.

APPENDIX C: VALIDITY AND REPLICABILITY STUDY

To enhance the validity and replicability of our Dictionaries (*PrivacyDIC* and *ConspiracyDIC*) we provide an additional analysis on two different datasets.

We collected tweets about the audio-solo social network "Clubhouse" to test the *PrivacyDIC* and tweets about "vaccines" to test the *ConspiracyDIC*. We retrieved tweets based on the hashtags #clubhouse and the keywords "clubhouse AND privacy" for the privacy data set and on the hashtag #vaccini for the vaccine data set. We streamlined our database removing retweets and tweets from verified users, resulting in a data set of 166 tweets about the audio-solo social network "Clubhouse" to test the *PrivacyDIC* and 1311 tweets about "vaccines" to test the *ConspiracyDIC*.

We have chosen Clubhouse because it represents a well-chosen case of privacy issues since it has been accused to lack some basic privacy safeguards needed according to the EU's General Data Protection Regulation (GDPR) (more info here: https://www.wired.co.uk/article/clubhouse-app-privacy-security). On the same vein, "vaccines" represents a well-chosen case of conspiracy theories as well. In fact, during the last two months Italy started the vaccine campaign rising conspiracy and no-vax debates on social media against the so-called "big Pharma", which was accused to impose the vaccine with the only aim of increasing profits.

We collected tweets in Italian, since *PrivacyDIC* and *ConspiracyDIC* are in Italian. Noteworthy, we selected two different contexts for privacy concerns and conspiracy theories since, when the authors conducted these further analyses, no context including both privacy concerns and conspiracy theories was available.

We included the two dictionaries *PrivacyDIC* and *ConspiracyDIC* in LIWC (Linguistic Inquiry and Word Count; Tausczik & Pennebaker, 2010) and performed the automated text analysis on the whole set of 166 tweets for Clubhouse and 1311 for vaccines tweets. We also included in the analysis the LIWC categories related to *text complexity*, word count (*wordcount*), presence of prepositions (*prepositions*), words with more than six letters (*six letters*) and cognitive mechanisms (*cognitive mechanisms*). To account for *certain language*, we included words communicating tentativeness (*tentative)* and certainty (*certainty*). To account for *emotions*, we included negative and positive emotions (*negative emotions* and *positive emotions*, respectively).

C.1 First data set

Regarding the Clubhouse data set, we estimated a Poisson model on the retweet count of the 166 tweets. We used the number of retweets as the dependent variable, *PrivacyDIC*, *ConspiracyDIC* and text complexity, certain language and emotions as independent variables. We also added the tweeter's characteristics and the presence of media elements as controls. To test hypotheses H1-H5 we calculated the full Model 8. Models 1-7 provide partial model estimates. In particular, we first calculated the intercept model, taken as a base model for further comparisons (Model 1). Then, we calculated Model 2 using PrivacyDIC (H1) and ConspiracyDIC (H2), Model 3 using text complexity (H3), Model 4 using certain language (H4) and Model 5 using emotions (H5). Model 6 includes all hypotheses-related variables and finally, Model 7 includes only the control variables. Table C1 below reports the results of our Poisson analysis using standardized variables. The differences between the full model and all the sub-models are significant (P(χ2, df)<1e-03).

C.2 S data set

Regarding the vaccine data set, we estimated a Poisson model on the retweet count of the 1311 tweets. We used the number of retweets as the dependent variable, *PrivacyDIC*, *ConspiracyDIC* and text complexity, certain language and emotions as independent variables. We also added the tweeter's characteristics and the presence of media elements as controls. To test hypotheses H1-H5 we calculated the full Model 8. Models 1-7 provide partial model estimates. In particular, we first calculated the intercept model, taken as a base model for further comparisons (Model 1). Then, we calculated Model 2 using PrivacyDIC (H1) and ConspiracyDIC (H2), Model 3 using text complexity (H3), Model 4 using certain language (H4) and Model 5 using emotions (H5). Model 6 includes all hypotheses-related variables and finally, Model 7 includes only the control variables. Table C2 below reports the results of our Poisson analysis using standardized variables. The differences between the full model and all the sub-models are significant (P(χ2, df) <1e-03).

C.3 Discussion

In both cases, in Model 8, *PrivacyDIC* is significant and negative, indicating that the inclusion of privacy concerns in the text may inhibit the diffusion of the tweet, providing an interesting and counterintuitive partial support to hypothesis H1. Meanwhile, *ConspiracyDIC* is significant and positive, indicating that the inclusion of conspiracy theories appeals to users, supporting H2.

C.4 Testing the external validity

To further support the external validity of our methodology, we validated the dictionaries with a survey. To do so, we extracted a sub-sample of 30 tweets with high level of privacy (according to *PrivacyDIC*) from the Clubhouse set of tweets; and a sub-sample of 30 tweets with high level of conspiracy (according to *ConspiracyDIC*) from the "vaccine" set of tweets. We considered "high-level" a rating greater than the 95% quantile of the distribution. Each participant evaluated 24 tweets on average (95% conf. interval: 22.7-25.3). We obtained an average level of agreement of .85% (95% conf. interval:- 0.81–0.89) for the Clubhouse tweets containing privacy concerns according to our *PrivacyDIC*; and an average level of agreement of .85% (95% conf. interval: .82 - .89) for the "vaccine" tweets containing conspiracy theories according to our *ConspiracyDIC*. These results are in line with those obtained on the original data set. Consistent to Humpreys and Wang (2018) we concluded that the high level of agreement obtained between computer-coded results with human-coded results supports also the external validity and replicability of our *PrivacyDIC* and *ConspiracyDIC*.

TABLE C1 Poisson Analysis “Clubhouse tweets”

	Dependent variable: retweet count							
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
ConspiracyDIC		0.373***				0.377***		0.508***
		(0.046)				(0.055)		(0.059)
PrivacyDIC		−0.345***				−0.010		−0.062
		(0.083)				(0.096)		(0.104)
Wordcount			0.527***			0.461***		0.501***
			(0.074)			(0.088)		(0.106)
Prepositions			−0.330***			−0.255**		−0.249**
			(0.092)			(0.103)		(0.114)
Six letter			−0.013			−0.089		−0.039
			(0.076)			(0.091)		(0.099)
Cognitive mechanisms			−0.226***			−0.015		0.082
			(0.086)			(0.085)		(0.093)
Tentative				−0.437***		−0.140		−0.150
				(0.108)		(0.135)		(0.136)
Certainty				−0.520***		−0.377**		−0.354**
				(0.143)		(0.164)		(0.160)
Positive emotions					0.092**	0.180***		0.060
					(0.047)	(0.053)		(0.053)
Negative emotions					−0.548***	−0.170		−0.011
					(0.102)	(0.121)		(0.127)
followers_count							0.361***	0.330***
							(0.093)	(0.125)
Friends_count							0.294***	0.459***
							(0.067)	(0.083)
statuses_count							−1.036***	−1.346***
							(0.244)	(0.313)
my. urls_urlyes							0.316	0.419
							(0.280)	(0.294)
media_typephoto							0.655***	0.093
							(0.153)	(0.193)
Constant	0.130*	−0.050	−0.065	−0.065	−0.004	−0.323***	−0.658**	−1.152***
	(0.073)	(0.084)	(0.087)	(0.093)	(0.084)	(0.109)	(0.285)	(0.301)
Observations	166	166	166	166	166	166	166	166
Log Likelihood	−357.790	−317.035	−322.972	−332.496	−336.747	−283.488	−317.561	−245.298
Akaike Inf. Crit.	717.581	640.070	655.945	670.991	679.494	588.976	647.122	522.596

Note: *$p < .1$; **$p < .05$; ***$p < .01$.

TABLE C2 Poisson Analysis "vaccine tweets"

	Dependent variable: retweet_count							
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
ConspiracyDIC		0.075***				0.063***		0.061***
		(0.015)				(0.016)		(0.016)
PrivacyDIC		−0.128***				−0.131***		−0.142***
		(0.023)				(0.025)		(0.025)
Word count			0.301***			0.332***		0.329***
			(0.018)			(0.018)		(0.018)
Prepositions			−0.232***			−0.238***		−0.283***
			(0.019)			(0.019)		(0.019)
Six letters			−0.200***			−0.205***		−0.209***
			(0.019)			(0.019)		(0.019)
Cognitive mechanisms			0.140***			0.175***		0.154***
			(0.017)			(0.018)		(0.019)
Tentative				−0.009		−0.074***		−0.078***
				(0.017)		(0.019)		(0.019)
Certainty				−0.191***		−0.265***		−0.276***
				(0.022)		(0.024)		(0.024)
Positive emotions					−0.070***	−0.103***		−0.102***
					(0.020)	(0.022)		(0.023)
Negative emotions					0.035**	−0.020		−0.022
					(0.016)	(0.017)		(0.018)
followers_count							0.187***	0.200***
							(0.009)	(0.009)
friends_count							0.219***	0.250***
							(0.019)	(0.021)
statuses_count							−0.143***	−0.155***
							(0.024)	(0.025)
my. urls_urlyes							−0.548***	−0.552***
							(0.037)	(0.039)
media_typephoto							0.161***	0.126***
							(0.037)	(0.038)
media_typephoto, photo							−15.392	−13.330
							(773.784)	(284.659)
Constant	1.009***	0.999***	0.923***	0.994***	1.006***	0.880***	1.132***	1.006***
	(0.017)	(0.017)	(0.018)	(0.017)	(0.017)	(0.019)	(0.024)	(0.027)
Observations	1,311	1,311	1,311	1,311	1,311	1,311	1,311	1,311
Log Likelihood	−8,309.727	−8,278.499	−8,008.389	−8,263.913	−8,300.672	−7,879.356	−8,006.671	−7,571.075
Akaike Inf. Crit.	16,621.450	16,563.000	16,026.780	16,533.830	16,607.340	15,780.710	16,027.340	15,176.150

Note: *$p < .1$; **$p < .05$; ***$p < .01$.