


Spreading Disinformation on Facebook: Do Trust in Message Source, Risk Propensity, or Personality Affect the Organic Reach of “Fake News”?

Tom Buchanan¹  and Vladlena Benson²

Social Media + Society
October–December 2019: 1–9
© The Author(s) 2019
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/2056305119888654
journals.sagepub.com/home/sms


Abstract

There is considerable concern about the propagation of disinformation through social media, particularly for political purposes. “Organic reach” has been found to be important in the propagation of disinformation on social networks. This is the phenomenon whereby social media users extend the audience for a piece of information: interacting with it, or sharing it with their wider networks, greatly increases the number of people the information reaches. This project evaluated the extent to which characteristics of the message source (how trustworthy they were) and the recipient (risk propensity and personality) influenced the organic reach of a potentially false message. In an online study, 357 Facebook users completed personality and risk propensity scales and rated their likelihood of interacting in various ways with a message posted by either a trustworthy or untrustworthy source. Message source impacted on overall organic reach, with messages from trusted sources being more likely to be propagated. Risk propensity did not influence reach. However, low scores on trait agreeableness predicted greater likelihood of interacting with a message. The findings provide preliminary evidence that both message source and recipient characteristics can potentially influence the spread of disinformation.

Keywords

organic reach, social media, personality traits, fake news, disinformation, Facebook

“Fake news” has been defined as disinformation spread through the media and then propagated through peer-to-peer communication (Albright, 2017). In this article, we consider the spread of disinformation through social media, specifically Facebook.

Much recent media discourse and political attention around fake news has focused on disinformation aimed at influencing political processes (BBC, 2018; European Commission, 2018). It has been characterized as a significant threat to democracy (House of Commons Digital, Culture, Media and Sport Committee, 2019). Examples of political disinformation activity that have seen considerable media coverage relate to the 2016 US presidential election, the 2016 UK referendum on leaving the European Union, and the 2018 Brazilian presidential election. Disinformation is also considered a problem across a number of other areas of society (e.g., medical or scientific disinformation, relating to vaccination or climate change). Many Americans now see “made-up news and information” as a critical problem, with a recent Pew Research Center survey finding more people

rated it as a “very big problem for the country” than violent crime, climate change or terrorism (Mitchell et al., 2019).

A typical definition of disinformation is “the deliberate creation and sharing of false and/or manipulated information that is intended to deceive and mislead audiences, either for the purposes of causing harm, or for political, personal or financial gain” (House of Commons Digital, Culture, Media and Sport Committee, 2018). This is distinct from “misinformation,” which is where individuals share false information in the mistaken belief that is actually true.

Material that is created with malicious intent may thus be spread innocently by other people through their social networks. For example, Howard et al.’s (2018) analysis of the

¹University of Westminster, UK

²Aston University, UK

Corresponding Author:

Tom Buchanan, School of Social Sciences, University of Westminster, 115 New Cavendish Street, London W1W 6UW, UK.
Email: T.Buchanan@westminster.ac.uk



Russian ‘Internet Research Agency’(IRA) disinformation group’s activity concludes that “over 30 million users, between 2015 and 2017, shared the IRA’s Facebook and Instagram posts with their friends and family, liking, reacting to, and commenting on them.” Indeed, there have been claims that disinformation seeded to a few thousand social media users during the 2016 US presidential election may have been propagated to hundreds of millions of people, vastly amplifying its scope for influence (Timberg, 2017).

This is the phenomenon of *organic reach* (Facebook, 2019). Through users’ interactions with the content (sharing it, liking it, and responding to it with comments on their timeline) they make other people within their wider networks aware of it. The extent to which users respond to a message influences the likelihood of that message being propagated into the newsfeed of other members of their social network. Thus, the behavior of individuals seeing disinformation can lead to an exponential spread of the false material. In fact, analysis by Vosoughi et al. (2018) indicated that false material spread on Twitter “farther, faster, deeper, and more broadly than the truth” and that this was primarily due to human behavior rather than the operation of bots. The scale of this phenomenon, and the risks it poses to society, make it important to consider why people spread false information they have seen online.

Disinformation as Cybercrime

In this project, we conceptualized the creation of online disinformation as a form of cybercrime. Those who initially create and seed it to social media networks are criminals (including hostile state actors). Those who encounter the material online and spread it further are essentially victims, duped by the message originators into spreading lies.

So why do individuals fall victim? The literature on different types of cybercrime includes examination of factors that may put people at risk of victimization (Benson & McAlaney, 2019). For example, Vishwanath et al. (2011) considered individual differences in vulnerability to phishing. In phishing, fraudsters send fake emails to individuals, trying to get them to reveal data such as passwords or personal information that can be used to attack them or their employers. Vishwanath et al. found that individuals’ habitual patterns of media use were an important risk factor for phishing. Buchanan and Whitty (2014) examined risk factors for online romance scams, where criminals develop electronically mediated (fake) romantic relationships with their victims, with the end goal of defrauding them. They found that individual differences in romantic beliefs were associated with the likelihood of being a victim. Research has not previously examined risk factors for being duped by “fake news.” However, there are some known general factors that could be important in this situation.

Extant research indicates that *trust* and *risk propensity* are among the factors that impact cyber-victimization of

individuals (Saridakis et al., 2016; Williams et al., 2017). Do these factors also determine whether we are likely to be fooled into propagating disinformation? And what other variables might increase the likelihood of someone mistakenly spreading false material online? This question is particularly important, given analysis by Guess et al. (2019) that indicated that fewer than 10% of Facebook users spread information from “fake news” domains. What sets these individuals apart from the 90% who did not?

Trust

This study follows a broad definition of trust, expressed as a willingness of one party (the trustor) to rely on another party (the trustee) in cases that involve risk and potential loss to the trustor (Gefen et al., 2003). Willingness to rely is driven by the judgment of the trustee’s characteristics (e.g., that the trustee has nothing to gain by deception). It has been shown that trust in virtual communities and teams increases knowledge sharing and information flow (Watson-Manheim & Bélanger, 2007). In the context of sharing news information online, there is evidence that individuals are more likely to trust, and engage with, a story when it is shared by someone they have a higher level of trust in (Sterret et al., 2018). Thus, we hypothesize that users will be more likely share information coming from a trusted source.

Risk Propensity and Cyber-Victimization

People are known to vary in the extent to which they are willing to accept risk in everyday life (Meertens & Lion, 2008). There are indications that social media users with high levels of risk propensity are more likely to become victims of cybercrime (Saridakis et al., 2016; Whittle et al., 2013). This is relevant to this project, because use of social media may involve a degree of risk (e.g., to security of one’s personal data). For example, Hajli and Lin (2016) discuss how information shared online could “rapidly become profiles and fodder for business purposes without users’ knowledge” (p. 111) and argue that sharing personal or private information online makes one vulnerable to scams and identity theft. Krombholz et al. (2015) describe ways in which the information people post to social media can be exploited in social engineering attacks, such as targeted “social phishing.” In such attacks, information specific to the victim is used to increase the effectiveness of phishing emails by making them appear to come from a friend. Thus, through social network usage, individuals engage in risk-taking behavior which involves communication with unknown entities, exchanging personal content and media, as well as providing and propagating sensitive information.

It has been known for some time that individuals’ level of acceptance of risk is associated with their use of social media. For example, Fogel and Nehmad (2009) showed that

individuals who used social media had higher levels of risk acceptance than those who did not. Of course, the social media landscape, and ubiquity of use, has changed since the time that work was done. However, there is regular media coverage of the risks that can be posed by social network sites such as Facebook. Individuals' awareness and acceptance of these risks will still influence their social media behavior. For example, Hajli and Lin (2016) found that social network users' perceptions of privacy risk influenced their attitude toward sharing information online. People who judged information sharing as being more risky had less positive attitudes toward it.

There are good reasons for this. The information you share online—for example, the posts you share on your own timeline—can have consequences. For instance, postings may be seen as unacceptable by powerful others such as future employers (Miller & Melton, 2015). This can extend to other types of interaction with online material. Marder et al. (2016) found that intention to publicly “like” a political party's page was inhibited by social anxiety related to the impression that this would present to others. Thus, the things we do and say online can be risky, and as social media users we are aware of this.

On the basis of such findings, we argue that people who have little appetite for risk would be less likely to share or visibly interact with material that might be controversial, or disapproved by others. Disinformation is, by its very nature, designed to provoke controversy. Thus, individuals high in risk propensity might be more likely to interact with disinformation items and thereby extend their organic reach. Conversely, those who are more risk-averse might be more likely to simply ignore such messages and not contribute to their propagation.

Personality Traits

Beyond risk propensity, other individual characteristics may influence the likelihood of interacting with fake news items. The personality profiles of Facebook users are of special interest here. The Five Factor Model (Costa & McCrae, 1992) delineates five main dimensions of individual differences in personality. Briefly, Extraversion influences preference for, and behavior in, social situations. Agreeableness reflects how friendly, trusting, and cooperative we tend to be in our interactions with others. Conscientiousness reflects reliability, organization, and methodical pursuit of goals. Neuroticism reflects the tendency to experience negative affect. Openness to Experience reflects “open mindedness” and interest in culture. There is evidence that an individual's status on all of these dimensions can be inferred from their social media footprint (e.g., Azucar et al., 2018; Hinds & Joinson, 2019). This implies that all of these personality dimensions have an influence on how we behave in social media.

For example, Extraversion is related to the number of Facebook friends a user has, Agreeableness to the type of

affect (positive or negative) expressed in status updates, Conscientiousness to the presence of political material in status updates, Neuroticism to frequency of posting, and Openness to Experience is related to the sharing of various forms of media (Hall et al., 2013). In terms of information-sharing behavior, Openness to Experience is positively associated, and Neuroticism negatively associated, with users' self-reports of the breadth of their self-disclosure on Facebook. In addition, Extraversion is positively associated with depth of self-disclosure (Hollenbaugh & Ferris, 2014). Such findings suggest that some personality characteristics might indeed influence our likelihood of interacting with disinformation items in social media, and thus their organic reach.

Hypotheses

The key dependent variable of interest in this study is the likelihood of a user propagating “fake” information through the organic reach phenomenon. Based on our conceptualization of social network users as potential cybercrime victims, we hypothesize that users who trust the originator of a message would be more likely to act in ways that increase its organic reach (H1). Thus, “fake news” items coming from trusted sources would be more likely to be propagated by the message recipients. Measuring trust can be problematic, as it is context-contingent and subjective (Sherchan et al., 2013). We need to define who and what the user is placing their trust in. Therefore, in this study the role of trust is tested through an experimental manipulation using two conditions: one where the source of a message is a trusted source (close friend), and another where they are a relatively unknown node in their social network.

Based on what is known about risk propensity and cybercrime victimization, we further hypothesize that people higher in risk propensity would be more likely to extend the organic reach of such messages (H2). We will also perform exploratory analyses of whether recipients' personality traits influence their likelihood of extending the organic reach of a message.

Method

Materials

The study was conducted online using an established personality testing website, and the Qualtrics online research platform. Participants were recruited, and personality and demographic data collected, through the personality testing website, www.personalitytest.org.uk. Participants were not directly recruited, but were referred by other sites or found it through search engines. The site hosted a 41-item personality questionnaire that provided measures of Extraversion, Neuroticism, Openness to Experience, Agreeableness, and Conscientiousness. This has been validated for use on the

Table 1. Indices of Organic Reach of a Facebook Posting.

How likely would you be to share it to your own public timeline?
How likely would you be to “like” it?
How likely would you be to comment on it (whether positively or negatively)?
How likely would you be to react to it by posting an emoji?

internet (Buchanan et al., 2005) and correlates well with the dimensions of Costa and McCrae’s (1992) model. Risk propensity was measured using Meertens and Lion’s (2008) Risk Propensity Scale, a seven-item measure addressing generalized tendencies to take risks in one’s everyday life. It has acceptable reliability, and has been used successfully in an online format (Branley & Covey, 2017).

The level of trust in the source of a potential “fake news” message was manipulated using a brief scenario. In the high-trust condition, the scenario read as:

In the run-up to an important national election, stories are circulating on Facebook about allegations of corruption against one of the candidates. A close friend who you know very well has made a post about it on their Facebook timeline, and asked all their friends to share it

In the low-trust condition, the scenario was identical except for the source of the message who was described as “Someone who recently send you a friend request, but who you do not really know.” While the topic of the post described was typical of those that might be fake news, there was no explicit indication as to whether the posting represented a truthful communication or not (as would be the case in real life). As a manipulation check, participants were asked to rate how likely they would be to “trust information posted by someone like that.”

Interaction with Facebook content was measured with indices of four ways users can respond to postings, all of which contribute to the organic reach of a posting. “Reactions” (including “likes”), “comments,” and “shares” are the standard metrics available for Facebook page posts. The Facebook actions of like, share, and comment can be seen as aspects of “electronic word-of-mouth” (Liu et al., 2017). Different message characteristics have been found to be associated with these distinct communication behaviors (Kim & Yang, 2017). While Facebook’s algorithms assign different weights to each of these user behaviors in determining whether a user’s audience sees the post they are responding to, it is clear that all contribute to the organic reach of a posting. Therefore, we asked participants to rate their likelihood of interacting with the purported Facebook posting in four different ways, as shown in Table 1.

Procedure

Individuals accessing the personality testing website first saw information about the study, gave consent, then answered the personality and demographic items. They then saw feedback

on their scores on each of the scales. Respondents consenting for their data to be used for research purposes then saw an invitation to proceed to the second stage of the study, described as a project looking at factors that influence how we interact with content posted on Facebook. Those following the link to the second part then completed the Risk Propensity Scale. They were then asked whether they used Facebook at all. Of those who did, half were then randomly assigned to see the high-trust version of the scenario, and the other half saw the low-trust version. They then completed the manipulation check item, and the four items measuring interactions with Facebook content.

Data Screening and Processing

The Qualtrics questionnaire was accessed by 441 individuals, of whom 420 went on to participate. Of these, 415 gave consent for their data to be analyzed. For ethical reasons, 6 individuals giving their age group as below 16 were removed. Qualtrics’ proprietary technology was used to prevent multiple completions, and the dataset was screened for unrealistic combinations of demographic data. The final sample comprised 409 individuals, of whom 357 were Facebook users. Sample sizes are lower for some analyses presented below, due to small amounts of missing data on some variables where participants omitted questions.

Participants

The demographics for all 409 participants are shown in Table 2. Respondents came from 44 different countries, with the greatest portion coming from the United States, followed by the United Kingdom. While there was considerable heterogeneity among participants, the majority were relatively young female students based in the United States, university or college-educated, who were participating as part of some educational activity. The great majority (357) were Facebook users. Further analyses were restricted to this subset of the sample, given that non-users would not be in a position to provide good-quality data about Facebook behaviors.

Results

Descriptive statistics for the risk propensity and personality scales are shown in Table 3. Among those participants who used Facebook, the four items indexing organic reach (share, like, comment, and react) intercorrelated sufficiently to form a scale with acceptable reliability. A total score for organic

Table 2. Demographic Data.

N	409
Sex	
Men	129 (31.5%)
Women	268 (65.5%)
Unanswered	12 (2.9%)
Age	
Modal age group	16–20 (25.7%)
Age range	16–80
Unanswered	0 (0%)
Location	
USA	221 (54.0%)
UK	50 (12.2%)
Other	132 (32.3%)
Unanswered	6 (1.5%)
Do you use Facebook at all?	
Yes	357 (87.3%)
No	45 (11.0%)
Prefer not to answer	7 (1.7%)
Route to participation	
Doing as part of some class	154 (37.7%)
Found through search engine	130 (31.8%)
Got link from a friend	24 (5.9%)
Followed link from another site	29 (7.1%)
Other	72 (17.6%)
Unanswered	0 (0%)
Highest level of education	
Less than high school	13 (3.2%)
High school/secondary school or equivalent	94 (23.0%)
Vocational/technical school or college	15 (3.7%)
Some college/university	122 (29.8%)
College/university graduate	82 (20.0%)
Some postgraduate	33 (8.1%)
Postgraduate/professional degree	50 (12.2%)
Unanswered	0 (0%)
Occupation	
Employed for wages	154 (37.7%)
Self-employed	26 (6.4%)
Unemployed	18 (4.4%)
Homemaker	9 (2.2%)
Student	170 (41.6%)
Retired	17 (4.2%)
Unable to work	6 (1.5%)
Unanswered	9 (2.2%)

Percentages may not sum exactly to 100% due to rounding errors.

reach was thus calculated by summing these four items and is also included in Table 3.

As a manipulation check, the item “how likely would you be to trust information posted by someone like that” was compared across the high-trust and low-trust conditions. As predicted, participants reported a higher likelihood of trusting the information in the high-trust condition ($M=2.47$, $SD=1.09$) than in the low-trust condition ($M=1.69$, $SD=.92$).

This difference was statistically significant ($t_{(349,65)}=-7.34$, $p<.0005$, using adjusted degrees of freedom due to a significant Levene’s test for equality of variance across conditions). This indicates that the trust manipulation was effective, and the two conditions differed in the extent to which the information source described was considered trustworthy by participants. Thus, condition was used as a predictor variable in the analysis of determinants of organic reach.

Multiple regression analysis was used to test the hypothesis that level of trust in the message originator, and individual differences in the recipient, would influence organic reach. Risk propensity and trust condition, plus the five personality variables, were used as predictors. The analysis, summarized in Table 4, indicated there was a statistically significant effect of trust manipulation on organic reach, with a higher level of reach for posts in the higher trust condition. Beyond this, only Agreeableness had a statistically significant effect on organic reach. Agreeableness was negatively associated with reach: less agreeable people were more likely to increase the message’s reach.

Discussion

As hypothesized, trustworthiness of the source of a message was associated with its potential organic reach. People rated themselves as more likely to extend the reach of a message coming from a trustworthy friend by sharing, liking, and so on. This is consistent with Williams et al.’s (2017) proposal that trust in a message source increases our vulnerability to online influence, for example, in the context of internet scams. It also chimes with Sterret et al.’s (2018) finding that trust in the source of information influences the extent to which we interact with it. At $\beta=.22$, the effect size exceeded the .2 threshold proposed for an effect that would have real-world significance (Ferguson, 2009). Thus, the effect may well have practical significance: disinformation is more likely to be propagated on Facebook if it reaches one from a trusted, rather than untrusted, source.

The hypothesized effect of risk propensity on organic reach of fake news was not found. The study was sufficiently powered to detect such an effect if it existed. Other factors, notably the extent to which one trusts the message source, are more likely to be important. This suggests that being tricked into spreading false information online differs in at least one way from other forms of cybercrime victimization. It may well be that sharing or liking a story on Facebook is seen as a low-risk activity, especially if it is believed to be true. This might be quite different from deciding to respond to a potential scam message, where one’s appetite for risk might be more influential.

Personality variables were included in the analysis on an exploratory basis. Of the five dimensions included, four had no effect on the measure of potential organic reach, suggesting that they may not affect this particular aspect of social

Table 3. Descriptive Statistics for Personality Scales, Risk Propensity, and Organic Reach.

Variable	N	M	SD	α	Range		Skew
					Potential	Actual	
Extraversion	409	27.76	7.50	0.86	9–45	10–45	-0.17
Agreeableness	409	28.07	4.37	0.74	7–35	13–35	-0.92
Conscientiousness	409	34.73	7.60	0.85	10–50	11–50	-0.47
Neuroticism	409	22.18	7.71	0.88	8–40	8–40	0.29
Openness to experience	409	27.46	5.20	0.75	7–35	9–35	-0.64
Risk propensity	406	28.90	10.24	0.77	7–63	7–54	0.14
Organic reach	355	7.10	3.49	0.80	4–20	4–20	1.13

SD: standard deviation.

Table 4. Effect of Trust Condition, Personality, and Risk Propensity on Organic Reach.

	B	SE	β	t	p
Constant	9.70	2.39		4.06**	.000
Risk propensity	0.00	0.02	.01	0.20	.843
Extraversion	0.03	0.03	.07	1.20	.231
Agreeableness	-0.12	0.05	-.15	-2.60*	.01
Conscientiousness	-0.03	0.03	-.07	-1.05	.295
Neuroticism	0.02	0.03	.04	0.51	.61
Openness to experience	-0.01	0.04	-.02	-0.29	.77
Trust condition	1.55	0.36	.22	4.31**	.000
R^2			.081		
F			4.33**		.000

SE: standard error.

Trust condition is coded as dummy variable: higher trust = 1, lower trust = 0.

* $p < .05$.

** $p < .0005$.

media behavior. The only personality variable found to affect the potential reach of a Facebook posting was Agreeableness. More agreeable people gave lower organic reach scores, and so were less likely to contribute to the propagation of a fake news item. The current dataset does not allow us to say whether this effect would apply to all fake news items, or is particular to the item described here. It might be that less agreeable people were more likely to propagate this story because it was negative in nature, alleging corruption against a political candidate. More agreeable people may have been less keen to interact with the post because it was inconsistent with their general friendly outlook.

This relationship must be treated as an exploratory observation. It requires replication, with different experimental stimuli, to establish that it is not a spurious finding. However, if it is genuine, then it may have concrete implications. If the effect is generalizable, then one could hypothesize that individuals or organizations wishing to propagate fake news on Facebook would do well to target their communications to people low on Agreeableness. There is evidence that this would be feasible, as Agreeableness is known to be detectable from social media footprints (Azucar et al., 2018). While the effect size is low, when operating at the massive scale made possible by social media, the effect has potential real-world

significance. As an example, work by Matz et al. (2017) has shown that personality-targeted advertising on social media can indeed influence user behavior.

Implications for Policy and Practice

The present findings point to potential strategies for spreading disinformation. Given that material coming from a trusted source is more likely to be interacted with, the originators of disinformation could leverage the effects of organic reach and amplify their message by making it appear to come from a trustworthy source. It is pertinent to note that in 2018, Twitter identified fraudulent accounts set up by a group linked to disinformation, which simulated those of US local newspapers (Mak & Berry, 2018). There is evidence that Americans trust such news sources more than national media (Mitchell et al., 2016). These appear to have been sleeper accounts established specifically for the purpose of building trust, just as envisioned in this scenario. Furthermore, if there are personality variables or other individual differences that increase vulnerability, then targeting individuals with the appropriate characteristics could again increase organic reach.

The same factors might inform the development of countermeasures for disinformation. Those users considered

vulnerable to disinformation campaigns could also be targeted by competing (truthful) messages, for example, debunking fake news articles. Finally, the principles could be put to work for prosocial ends. For example, identifying individuals likely to extend the organic reach of health-promotion messaging could be of value in amplifying socially useful information.

Limitations

One shortcoming of this study is that a single exemplar of a (potential) fake news item was used. Participant Agreeableness influenced the likely organic reach of that item. However, this could have been due to an interaction between that trait and the content of that specific item. It remains to be seen whether Agreeableness would also influence the organic reach of other types of material. Thus, replication with other materials is required.

Generalizability is also limited by the nature of the trust manipulation and the scenario used (an election campaign). The manipulation check established that the two conditions differed in the extent to which the source was seen as trustworthy. However, the level of trustworthiness was confounded with the likely reason that one source was trusted more than the other: closeness of the relationship with the source. It is possible that the closeness of the relationship was the key factor, and that people reported themselves as more likely to propagate material from a socially closer source, due to some sense of social obligation rather than trust. Thus replication with different trust manipulations is required. Finer grained comparisons are also desirable. The present manipulation compared two relatively distinct scenarios (close friend vs virtual stranger). Consideration of the different degrees of trustworthiness would be of value to establish the nature of the relationship.

The single scenario used (an election campaign) also limits generalizability. Trust is very much context dependent, and who one trusts may differ across different scenarios. Who one trusts with respect to political information, might be quite different to who one trusts with respect to other material (for instance, information concerning health, such as vaccine safety). Having said that, even if the present findings only apply to election campaigns, they may still have considerable importance given the significance of such events.

A further consideration is that in this study, given the use of a hypothetical scenario (about political corruption), the status of the “fake news story” as being either true or misleading information was never made clear to participants. In fact, this would normally be the situation in real life: individuals often have no way of knowing for sure whether information they come across is true. How they perceived its truthfulness, and whether their perception would have influenced their behavior, is an open question. It is worth noting a Pew Research Center survey that found believing a story was false was not necessarily a barrier to sharing it (Barthel et al.,

2016). Deliberate propagation of disinformation may offer individuals an opportunity to express a political affiliation or social identity, regardless of whether it is actually believed or not. The beliefs and motivations of the estimated 10% of Facebook users who do spread such information (Guess et al., 2019) require examination.

Another limitation is that the work reported here relies entirely on self-reported likelihood of interactions with material that would extend organic reach. Stronger evidence would come from actual behavioral observations: when presented with a (potentially) fake news item, does user personality predict whether they actually propagate it by liking or sharing? However, answering that question would present both ethical and practical issues around the use of real social media platforms as observational research environments.

Finally, the variables measured here accounted for only a small proportion of variance in the self-rated likelihood of propagating disinformation. Other, unmeasured, factors, are sure to play a role. Key among these are likely to be digital literacy, and the extent to which a specific disinformation message is consistent with the user’s own views and social or political identity. Other likely influences are the extent to which a person is interested in politics, and their general patterns of social media behavior (for example, are they typically active sharers of material posted by others).

Conclusion

While it has limitations, this study suggests that source and recipient characteristics could influence the likelihood of individuals propagating disinformation on social media. Evidence from other sources implies the feasibility of leveraging trust in message sources, and microtargeting disinformation to individuals based on individual differences, in order to amplify “fake news” through the phenomenon of organic reach. Given the potential high-stakes outcomes of such activity, further consideration is warranted.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Tom Buchanan  <https://orcid.org/0000-0002-8994-2939>

References

- Albright, J. (2017). Welcome to the era of fake news. *Media and Communication*, 5(2), 87–89. <https://doi.org/10.17645/mac.v5i2.977>

- Azucar, D., Marengo, D., & Settanni, M. (2018). Predicting the Big 5 personality traits from digital footprints on social media: A meta-analysis. *Personality and Individual Differences, 124*, 150–159. <https://doi.org/10.1016/j.paid.2017.12.018>
- Barthel, M., Mitchell, A., & Holcomb, J. (2016). *Many Americans believe fake news is sowing confusion*. http://assets.pewresearch.org/wp-content/uploads/sites/13/2016/12/14154753/PJ_2016.12.15_fake-news_FINAL.pdf
- BBC. (2018). *Beyond “fake news.”* <https://www.bbc.co.uk/mediacentre/latestnews/2018/beyond-fake-news>
- Benson, V., & McAlaney, J. (2019). *Cyber influence and cognitive threats*. Elsevier Academic Press.
- Branley, D. B., & Covey, J. (2017). Is exposure to online content depicting risky behavior related to viewers’ own risky behavior offline? *Computers in Human Behavior, 75*, 283–287. <https://doi.org/10.1016/j.chb.2017.05.023>
- Buchanan, T., Johnson, J. A., & Goldberg, L. R. (2005). Implementing a Five-Factor Personality Inventory for use on the Internet. *European Journal of Psychological Assessment, 21*(2), 115–127. <https://doi.org/10.1027/1015-5759.21.2.115>
- Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime and Law, 20*(3), 261–283. <https://doi.org/10.1080/1068316X.2013.772180>
- Costa, P. T., & McCrae, R. R. (1992). *Revised NEO Personality Inventory (NEO PI-R) and NEO Five-Factor Inventory (NEO FFI): Professional manual*. Psychological Assessment Resources.
- European Commission. (2018). *A Europe that Protects: The EU steps up action against disinformation*. http://europa.eu/rapid/press-release_IP-18-6647_en.htm
- Facebook. (2019). *What’s the difference between organic, paid and post reach?* <https://www.facebook.com/help/285625061456389?helpref=search&query=organic%20reach&sr=1&ref=contextual>
- Ferguson, C. J. (2009). An effect size primer: A guide for clinicians and researchers. *Professional Psychology: Research and Practice, 40*(5), 532–538. <https://doi.org/10.1037/a0015808>
- Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*(1), 153–160. <https://doi.org/10.1016/j.chb.2008.08.006>
- Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51. <https://doi.org/10.2307/30036519>
- Guess, A., Nagler, J., & Tucker, J. (2019). Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science Advances, 5*(1), eaau4586. <https://doi.org/10.1126/sciadv.aau4586>
- Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics, 133*(1), 111–123. <https://doi.org/10.1007/s10551-014-2346-x>
- Hall, J. A., Pennington, N., & Lueders, A. (2013). Impression management and formation on Facebook: A lens model approach. *New Media & Society, 16*(6), 958–982. <https://doi.org/10.1177/1461444813495166>
- Hinds, J., & Joinson, A. (2019). Human and computer personality prediction from digital footprints. *Current Directions in Psychological Science, 28*, 204–211. <https://doi.org/10.1177/0963721419827849>
- Hollenbaugh, E. E., & Ferris, A. L. (2014). Facebook self-disclosure: Examining the role of traits, social cohesion, and motives. *Computers in Human Behavior, 30*, 50–58. <https://doi.org/10.1016/j.chb.2013.07.055>
- House of Commons Digital, Culture, Media and Sport Committee. (2018). *Disinformation and “fake news”: Interim report: Government response to the Committee’s fifth report of session 2017–19*. <https://publications.parliament.uk/pa/cm201719/cmselect/cmcmds/1630/1630.pdf>
- House of Commons Digital, Culture, Media and Sport Committee. (2019). *Disinformation and “fake news”: Final Report*. <https://publications.parliament.uk/pa/cm201719/cmselect/cmcmds/1791/1791.pdf>
- Howard, P. N., Ganash, B., Liotsiou, D., Kell, J., & François, C. (2018). *The IRA, social media and political polarization in the United States, 2012–2018* (Working Paper 2018.2). <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/IRA-Report-2018.pdf>
- Kim, C., & Yang, S.-U. (2017). Like, comment, and share on Facebook: How each behavior differs from the other. *Public Relations Review, 43*(2), 441–449. <https://doi.org/10.1016/j.pubrev.2017.02.006>
- Kromholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, 113–122. <https://doi.org/10.1016/j.jisa.2014.09.005>
- Liu, J., Li, C., Ji, Y. G., North, M., & Yang, F. (2017). Like it or not: The Fortune 500’s Facebook strategies to generate users’ electronic word-of-mouth. *Computers in Human Behavior, 73*, 605–613. <https://doi.org/10.1016/j.chb.2017.03.068>
- Mak, T., & Berry, L. (2018). *Russian influence campaign sought to exploit Americans’ trust in local news*. <https://www.npr.org/2018/07/12/628085238/russian-influence-campaign-sought-to-exploit-americans-trust-in-local-news>
- Marder, B., Slade, E., Houghton, D., & Archer-Brown, C. (2016). “I like them, but won’t “like” them”: An examination of impression management associated with visible political party affiliation on Facebook. *Computers in Human Behavior, 61*, 280–287. <https://doi.org/10.1016/j.chb.2016.03.047>
- Matz, S. C., Kosinski, M., Nave, G., & Stillwell, D. J. (2017). Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the National Academy of Sciences of the United States of America, 114*(48), 12714–12719. <https://doi.org/10.1073/pnas.1710966114>
- Meertens, R. M., & Lion, R. (2008). Measuring an individual’s tendency to take risks: The Risk Propensity Scale. *Journal of Applied Social Psychology, 38*(6), 1506–1520. <https://doi.org/10.1111/j.1559-1816.2008.00357.x>
- Miller, R., & Melton, J. (2015). College students and risk-taking behaviour on Twitter versus Facebook. *Behaviour & Information Technology, 34*(7), 678–684. <https://doi.org/10.1080/0144929X.2014.1003325>
- Mitchell, A., Gottfried, J., Barthel, M., & Shearer, E. (2016). *The modern news consumer: News attitudes and practices in the digital era*. <http://www.journalism.org/2016/07/07/the-modern-news-consumer/>

- Mitchell, A., Gottfried, J., Fedeli, S., Stocking, G., & Walker, M. (2019). *Many Americans say made-up news is a critical problem that needs to be fixed*. <https://www.journalism.org/2019/06/05/many-americans-say-made-up-news-is-a-critical-problem-that-needs-to-be-fixed/>
- Saridakis, G., Benson, V., Ezingear, J.-N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change, 102*, 320–330. <https://doi.org/10.1016/j.techfore.2015.08.012>
- Sherchan, W., Nepal, S., & Paris, C. (2013). A survey of trust in social networks. *ACM Computing Surveys, 45*(4), 1–33. <https://doi.org/10.1145/2501654.2501661>
- Sterret, D., Malato, D., Benz, J., Kantor, L., Tompson, T., Rosenstiel, T., Sonderman, J., Loker, K., & Swanson, E. (2018). *Who shared it?: How Americans decide what news to trust on social media*. <http://www.norc.org/PDFs/Working%20Paper%20Series/WP-2018-001.pdf>
- Timberg, C. (2017). *Russian propaganda may have been shared hundreds of millions of times, new research says*. https://www.washingtonpost.com/news/the-switch/wp/2017/10/05/russian-propaganda-may-have-been-shared-hundreds-of-millions-of-times-new-research-says/?utm_term=.15912b814dc0
- Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576–586. <https://doi.org/10.1016/j.dss.2011.03.002>
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science, 359*(6380), 1146–1151. <https://doi.org/10.1126/science.aap9559>
- Watson-Manheim, M. B., & Bélanger, F. (2007). Communication media repertoires: Dealing with the multiplicity of media choices. *MIS Quarterly, 31*(2), 267. <https://doi.org/10.2307/25148791>
- Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of online grooming: Characteristics and concerns. *Aggression and Violent Behavior, 18*(1), 62–70. <https://doi.org/10.1016/j.avb.2012.09.003>
- Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior, 72*, 412–421. <https://doi.org/10.1016/j.chb.2017.03.002>

Author Biographies

Tom Buchanan (PhD, University of Aberdeen) is a Professor of Psychology at the University of Westminster, UK. His research interests include the psychology of “online behavior” and how people engage with online technologies.

Vladlena Benson (PhD, University of Texas at Dallas) is a Professor of Cybersecurity at Aston University, where she is the director of Cyber Security Innovation partnership and the Head of the IS research group. Her research interests include online victimization, behavioral analytics, cybersecurity risk management, and technology governance.