Navigating through real and fake news by using provenance information

Bianca Rodrigues Teixeira and Simone D. J. Barbosa
Department of Informatics, PUC-Rio R. Marques de Sao Vicente, 225, Rio de Janeiro, RJ 22451-900, Brazil
bteixeira@inf.puc-rio.br, simone@inf.puc-rio.br

Abstract

With the large number of internet users today, fake news and misinformation become more and more visible online, especially through social media platforms. Users' belief in online information and news is related to trust in the information sources. To prevent the dissemination of fake news and misinformation online, trust can be supported by provenance information in online publications. We use the OurPrivacy conceptual framework to illustrate a way in which provenance can be used to help users define their trust in artifacts posted online. We also discuss the possibility to filter artifacts by only viewing trusted sources of information.

Keywords

Provenance · Trust · Fake News · Privacy · Conceptual Framework

---

How to cite this book chapter:
Rodrigues Teixeira, B. and Barbosa, S.D.J. 2020. Navigating through real and fake news by using provenance information. In: Loizides, F., Winckler, M., Chatterjee, U., Abdelnour-Nocera, J. and Parmaxi, A. (eds.) *Human Computer Interaction and Emerging Technologies: Adjunct Proceedings from the INTERACT 2019 Workshops*. Pp. 49–56. Cardiff: Cardiff University Press. DOI: https://doi.org/10.18573/book3.f.
License: CC-BY 4.0.

1 Introduction

Internet users are everywhere. Around the globe, smartphone ownership rates are rising fast [12], especially in developing countries in which mobile phones used to be considered a luxury. Because of the large amounts of active internet users, it is safe to say that fake news or misinformation online is more dangerous than ever. Although trusted organizations attract more direct traffic [13], Allcott and Gentzkow performed a study on the 2016 United States presidential election and found that 13.8% of news and information was accessed on social media [1]. More recently, in a study with 174 participants, Bentley et al. found that 16% of all news sessions started from social media [2]. The shareability of fake news in social media is massive, and in a recent survey, 37% of the respondents admitted having "come across a news story, believed it to be true, then later realized that it was either exaggerated, inaccurate or blatantly false" [6]. Moreover, people may remember fake news better than traditional news [3].

Besides social media, messaging mobile applications, such as WhatsApp, with over one billion active users [5], provide a great platform for the dissemination of all kinds of information, including misinformation. This issue is so well known that, on their Frequently Asked Questions page, WhatsApp provides tips to help prevent the spread of rumors and fake news [16]. They include a brief explanation of their "*Forwarded*" feature, which indicates whether a message has been forwarded to the user. This could mean that the person who sent it may not have written it, and thus the receiving end should double check the facts.

Lazer et al. discussed potential interventions for controlling the flow of fake news, dividing them into two categories: individual empowerment and algorithms [11]. The former includes mostly fact checking and researching as a means to confirm the information, whilst the latter regards automatic detection of untrustworthy sources. The authors suggest that social media platforms could provide a sort of "seal of approval" for certain sources, which then would be used to sort and rank the content the users would then consume.

In the following section we discuss some of the trust and provenance aspects of information shared online. Next, we propose to use a conceptual framework to help contain the flow of fake news. Finally, we provide a conclusion and propose next steps.

2 Provenance and trust

Gil and Artz define content trust as "a trust of judgement on *a particular piece of information* in a given context" [7]. It is a subjective judgment, and two people may have opposite opinions on whether they trust a piece of information. This generates a problem when it comes to actual false information. It is not possible to control whether someone will believe what he/she reads online, and

often people believe without questioning. In particular, older adults are more likely to believe false information than young adults, consciously recollecting false statements as true [3, 8]. Therefore, although there are indeed internet users who may believe false information more often than other users, it is still important to lower trust on fake news or misinformation.

Wang and Mark performed a study in 2013 comparing trust in official media and in citizen media in China [15]. Official media comprises companies run or influenced by the state, with professional journalists, and citizen media is media posted and disseminated by citizens in social media. They found two contrasting groups of respondents, Traditional (high trust in official, low trust in citizen media) and New Generation (low trust in official, high trust in citizen media). The authors hypothesize that this difference in behavior could be due to political views, or due to the social media adoption by the New Generation group, earlier than the Traditional group, which can lead to familiarity and then trust in citizen media.

In a similar study, Hermida et al. found that 37% of news consumers tend to trust and prefer content curated by professional journalists over user-generated content, but 44% of respondents were unsure [9]. Ultimately, on specific pieces of information, this uncertainty will result in either trust or not trust.

Gil and Artz listed 19 factors that influence content trust [7]. In this paper, in order to help users make a decision on trust, we focus on *provenance*. Provenance, in this context, can be defined as the source and date of a piece of information, such as a news outlet. News articles that are purposefully created as fake news usually are not originated from a source with respectful journalistic reputation, so their provenance may not generate trust on the reader.

The provenance of a piece of information has a direct effect on trust [6], which then defines whether a reader believes in it or not. When a news article is shared on social media, the provenance is easily identified by experienced users via the URL of the source website. However, when the information shared does not contain a clear source, the users have to do research and fact check it themselves, but this requires some skepticism from their part.

Content trust can also be established by having a "trust chain". One may not trust a specific piece of information published by an untrusted source A, but if a previously trusted source B states that it trusts A's publication, then one can then start trusting A [10].

In the next section, we discuss the use of a conceptual framework called OurPrivacy in the context of using provenance information to create – or not – trust in information shared online.

3 OurPrivacy

OurPrivacy is a conceptual framework to characterize what privacy is in the context of social networks and how privacy rules can be expressed [14]. Each

piece of information is modelled as a nanopublication,[1] which comprises three basic elements: the assertions, the provenance, and the publication information. The assertions are related to the content of the nanopublication, *i.e.*, the semantic information it represents. The provenance is considered metadata about the assertions: it contains information about how to assertions came to be. Finally, the publication information is metadata about the nanopublication as a whole. In the context of a social network, it contains information about the user who actively posted the nanopublication, whereas the provenance information regards where the information (assertions) actually came from.

By modeling social media artifacts as nanopublications, the provenance information can be used as a means to establish trust in that artifact. Having this information readily available, since it is tied to the content of the artifact, the user can use it to determine whether he/she trusts it or not.

OurPrivacy also allows users to create privacy rules. A privacy rule can reference the content (assertions), provenance or publication information of an artifact. For instance, John Stuart can specify a rule that states that he only wants to access artifacts that have BBC or CNN listed as their provenance. He can also set a rule that prevents his grandmother from viewing his publications about politics, maybe because he tends to use sarcastic tones and knows his grandmother would take his words literally.

The OurPrivacy framework allows for customization of rules about virtually any type of artifact, since we consider that the assertions would contain complete semantic information, which would be supported by the provenance information. This model could be used as a way to help control the dissemination of fake news or misinformation, by using the provenance information as a type of filter.

Besides being able to create rules in a top-down fashion, as stated above, we can also envisage using fake news detectors, such as XFake [17], to inform our decisions on which rules to create, thus also supporting a bottom-up process for creating rules.

The "trust chain" mentioned in the previous section can also be tracked using OurPrivacy in a network of artifacts. As an example, we have a user U, an untrusted source A and a trusted source B. A's publications are generally not trusted by U, whereas B's are trusted. If B were to publish a claim, *i.e.*, generate a new artifact, about trusting A's publication, in the "provenance" element of the artifact there would be some information relating to A's original publication. Since B is citing A's publication in order to back it up, the provenance information should contain A's publication. Also, in the assertions, it should be stated that B trusts A's publication.

This way, the user U could also customize rules or browse the network looking for trusted sources that claim to trust the previously untrusted publication

[1] http://nanopub.org/wordpress/.

by A. The chain of claims regarding trust in other publications should be transparent for users to help make their decisions about trusting new sources.

By modeling social media using nanopublications as artifacts, as proposed in OurPrivacy, a change in paradigm is impending. In social networks today, it is common to have both the assertion and the publication information components. The provenance aspect would be a new element, and social media users would need to be aware of the change. Publications and news they consume would have the provenance information available, and people would learn to use it to make more informed decisions regarding trust and whether to disseminate the publication.

4 Conclusions

The information available on social media today is mostly unstructured, which makes it difficult to track and to navigate in. This helps with the propagation of fake news, which are posted and consumed every day, especially in social media and messaging applications. The general population tends to use social media without considering the impact of their publications. Sharing misinformation is not usually seen as a critical act, but in our view it should.

The OurPrivacy conceptual framework can be used as a model for a more transparent social media. By mapping artifacts as nanopublications, the provenance information is tied with the assertions contained in the artifact, and can help the user in knowing the source of the information. Although most publications in social media today do not contain clear sources and are not structured in a way that contains semantic information, perhaps in the future this shall be possible, and OurPrivacy could be used to model this network.

Trust in information online varies from person to person, but we can try to make it easier for users to make their decisions when defining their beliefs. By providing clear provenance information, or allowing users to filter through their networks, we can perhaps help decrease the proliferation of fake news and misinformation.

References

1. Allcott, H., Gentzkow, M.: Social Media and Fake News in the 2016 Election. Journal of Economic Perspectives. 31, 211–236 (2017). https://doi.org/10.3386/w23089.
2. Bentley, F. et al.: Understanding Online News Behaviors. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. pp. 590:1–590:11 ACM, New York, NY, USA (2019). https://doi.org/10.1145/3290605.3300820.

3. Budak, C.: What Happened? The Spread of Fake News Publisher Content During the 2016 U.S. Presidential Election. In: The World Wide Web Conference. pp. 139–150 ACM, New York, NY, USA (2019). https://doi.org/10.1145/3308558.3313721.
4. Chen, Y.: Unwanted Beliefs: Age Differences in Beliefs of False Information. Aging, Neuropsychology, and Cognition. 9, 217–230 (2002). https://doi.org/10.1076/anec.9.3.217.9613.
5. Constine, J.: WhatsApp hits 1.5 billion monthly users. $19B? Not so bad., http://social.techcrunch.com/2018/01/31/whatsapp-hits-1-5-billion-monthly-users-19b-not-so-bad/.
6. Flintham, M. et al.: Falling for Fake News: Investigating the Consumption of News via Social Media. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. pp. 376:1–376:10 ACM, New York, NY, USA (2018). https://doi.org/10.1145/3173574.3173950.
7. Gil, Y., Artz, D.: Towards content trust of web resources. Journal of Web Semantics. 5, 227–239 (2007). https://doi.org/10.1016/j.websem.2007.09.005.
8. Grace, L., Hone, B.: Factitious: Large Scale Computer Game to Fight Fake News and Improve News Literacy. In: Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems. p. CS05:1–CS05:8 ACM, New York, NY, USA (2019). https://doi.org/10.1145/3290607.3299046.
9. Hermida, A., Fletcher, F., Korell, D., Logan, D.: Share, Like, Recommend: Decoding the social media news consumer. Journalism Studies. 13, 815–824 (2012). https://doi.org/10.1080/1461670X.2012.664430.
10. Laufer, C., Schwabe, D.: A Framework to Support the Trust Process in News and Social Media. In: Proceedings of the Workshop on Semantic Web for Social Good co-located with 17th International Semantic Web Conference (ISWC 2018). Monterey, CA, USA (2018).
11. Lazer, D.M.J., Baum, M.A., Benkler, Y., Berinsky, A.J., Greenhill, K.M., Menczer, F., Metzger, M.J., Nyhan, B., Pennycook, G., Rothschild, D., Schudson, M., Sloman, S.A., Sunstein, C.R., Thorson, E.A., Watts, D.J., Zittrain, J.L.: The science of fake news. Science. 359, 1094–1096 (2018). https://doi.org/10.1126/science.aao2998.
12. Poushter, J.: Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies | Pew Research Center, https://www.pewglobal.org/2016/02/22/smartphoneownership-and-internet-usage-continues-to-climb-in-emerging-economies/, (2016), last accessed 2019/04/20.
13. Taneja, H., Yaeger, K.: Do People Consume the News They Trust? In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. pp. 540:1–540:10 ACM, New York, NY, USA (2019). https://doi.org/10.1145/3290605.3300770.

14. Teixeira, B., Schwabe, D., Santoro, F., Baião, F., Campos, M.L., Verona, L., Laufer, C., Barbosa, S.D.J., Lifschitz, S., Costa, R.: Privacy and Transparency within the 4IR: Two faces of the same coin. In: Proceeding of FATES on the Web, co-located with The Web Conference '19., San Francisco, CA, USA (2019).
15. Wang, Y., Mark, G.: Trust in Online News: Comparing Social Media and Official Media Use by Chinese Citizens. In: Proceedings of the 2013 Conference on Computer Supported Cooperative Work. pp. 599–610. ACM, New York, NY, USA (2013). https://doi.org/10.1145/2441776.2441843.
16. WhatsApp FAQ - Tips to help prevent the spread of rumors and fake news, https://faq.whatsapp.com/en/26000216/?category=5245250, last accessed 2019/04/20.
17. Yang, F. et al.: XFake: Explainable Fake News Detector with Visualizations. In: The World Wide Web Conference. pp. 3600–3604 ACM, New York, NY, USA (2019). https://doi.org/10.1145/3308558.3314119.