MisVis: Explaining Web Misinformation Connections via Visual Summary

ANONYMOUS AUTHOR(S)

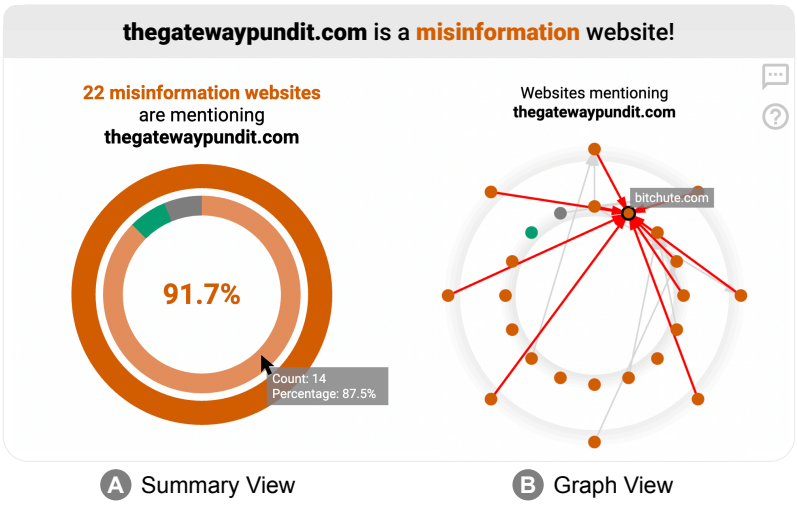

Fig. 1. **(A)** When a user visits a misinformation website (e.g., thegatewaypundit.com as verified by PolitiFact [3]), MisVis's Summary View shows the site's overall reliability by visualizing the distributions of its hyperlinked websites—22 of the 24 sites (91.7%) mentioning it are misinformation sites; *misinformation* sites shown in orange, *reliable* in green, and *unlabeled* in gray. **(B)** MisVis's Graph View reveals the connections among sites, such as the well-known misinformation website *bitchute.com* [14, 30] with a high degree of connections to other misinformation sites, serving as a "hub" in spreading misinformation.

Identifying and raising awareness about web misinformation is crucial as the Internet has become a major source of information for many people. We introduce MisVis, a web-based interactive tool that helps users better assess misinformation websites and understand their connections with other misinformation sites through visual explanations. Different from the existing techniques that primarily only focus on alerting users of misinformation, MisVis provides new ways to visualize *how* the site is involved in spreading information on the web and social media. Through MisVis, we contribute novel interactive visual design: Summary View helps users understand a site's overall reliability by showing the distributions of its linked websites; Graph View presents users with the connection details of how a site is linked to other misinformation websites. In collaboration with researchers at a large security company, we are working to deploy MisVis as a web browser extension for broader impact.

CCS Concepts: • **Human-centered computing** → **Visualization toolkits**.

Additional Key Words and Phrases: interactive visualization, web misinformation, toolkit

Manuscript submitted to ACM

ACM Reference Format:
Anonymous Author(s). 2022. MisVis: Explaining Web Misinformation Connections via Visual Summary . In *CHI '22: Late-Breaking Work, April 30–May 06, 2022, New Orleans, LA.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

With the exponential growth of information online, the Internet has become a major source of information for many people [26]. Unfortunately, *misinformation* mushrooms as well, affecting many aspects of life, from creating confusion and fear [13], inciting violence [12], to endangering life [27]. To curb misinformation, recent research has started to develop methods and tools to analyze how the inaccurate information spreads across the web [5, 7, 14, 19, 21, 22, 29]. Some efforts focus on checking the factualness of information. For example, Ciampaglia et al. [9] computationally fact-check information, while Snopes [4], FAIR [2], FactCheck.org [25], and PolitiFact [3] provide web-based fact-checking platforms to allow people to easily validate information. Web browser extensions have been developed to help identify misinformation on social media. For example, Bot Sentinel [17] constructs a machine learning classifier to detect inappropriate tweets, while Project Fib [23] detects fake news on Facebook. Ennals et al. [11] warn users about the misinformation on websites and social media. Herrmannova et al. [15] address the challenges in automating misinformation detection, while Eccles and Dingler [10] attempt to reduce fake news dissemination and consumption.

However, most existing techniques primarily focus on alerting people that a site may be spreading misinformation [9, 14, 17, 29]. Little research has been conducted on visually explaining how misinformation sites engage in spreading misinformation through its connections to other misinformation sites [14]. To fill this research gap, our ongoing work makes the following contributions:

- We present **MisVis**, a web-based interactive tool that provides new ways for users to better understand how a site is involved in spreading misinformation on world-wide-web and social media by visualizing its connections with other misinformation websites. MisVis complements existing techniques that primarily focus on detecting or alerting users of misinformation. In collaboration with researchers at a large security company, we are working to deploy MisVis as a web browser extension for broader impact. A demo video of MisVis is available as a video figure.
- **Novel interactive visual design of MisVis** provides two coordinated views for assessing a misinformation site. The Summary View helps users understand a site's overall reliability by visualizing the distributions of its hyperlinked websites (Figure 1A). The Graph View shows the connection details and potential flow of misinformation by visualizing how a site is linked to other misinformation websites (Figure 1B). Users can freely switch between the two coordinated views, with in-between animated transitions that communicate the two views' visual relationships (Figure 2).

2 SYSTEM DESIGN AND IMPLEMENTATION

2.1 Overview

We design MisVis as a lightweight interactive visualization that would display as the user visits a website, to help them understand how the site may be involved in spreading information on the web and social media. Formally, we call the site that the user is visiting the *target website*.

Data. MisVis makes use of two datasets: *domain* data and *Twitter users* data. The domain data was collected by Sehgal et al. [28], consisting of 2,118 web domains. Half of the domains are misinformation sites, curated from publicly available

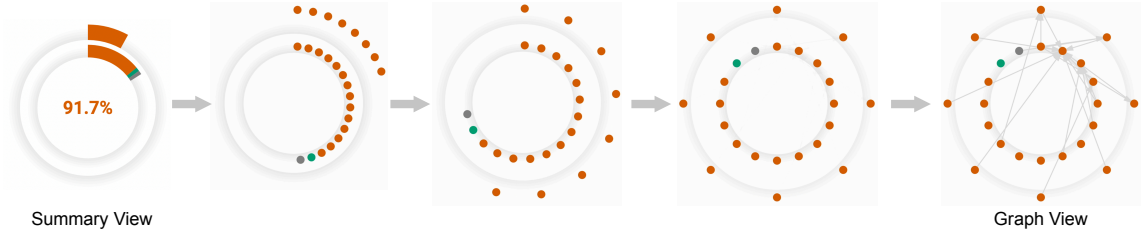

Fig. 2. Animation of the transition from Summary View (leftmost) to Graph View (rightmost). The rings (of the doughnut charts) are first replaced by the individual sites (nodes) that they represent, then the sites animate to spread out, finally the connections (edges) among the sites appear.

misinformation datasets; the other half are top-ranked reputable, informational domains on Alexa. For each domain, all the HTML hyperlink tags (`<a href="...">..</a>`) present on the page are scraped to generate the 1-hop network, which consists of all domains directly connected to the target site, and any links among them. The 2-hop network is created by scraping the hyperlink tags of each web page in the 1-hop network. For the sites' reliability, we use the original labels provided by Sehgal et al. [28], i.e., a site is labeled misinformation, reliable, or unlabeled. We acquired the Twitter users data by using Twitter's Search Tweets API [1], which allowed us to search for tweets based on shared URLs. We collected 99,141 unique Twitter users who recently shared URLs from at least one of the 2,118 sites in the domain dataset. To determine whether a Twitter user is a real person or a bot, we used the botometer-python API [2].

User Interface. Implemented using D3.js [6], MisVis runs in all modern web browsers. It consists of four components:

(1) **Header** displays a message for whether the target website is a misinformation site;
(2) **Main Window** (Figure 1) provides two coordinated views to help users understand a site's overall reliability and how it is involved in spreading information via its connections with other sites (Section 2.2);
(3) **Twitter User Window** (Figure 3) describes key characteristics of the Twitter users that have shared information from the target website (Section 2.3); and
(4) **Settings Panel** (Figure 4) allows users to switch between Summary View and Graph View, and configure their properties (Section 2.4).

2.2 Main Window

The Main Window (Figure 1) provides users with two coordinated views for assessing a misinformation site. The Summary View (Figure 1A) helps users understand a site's overall reliability by visualizing the distributions of its hyperlinked websites (Section 2.2.1). The Graph View (Figure 1B) shows the connection details and potential flow of misinformation by visualizing how a site is linked to other misinformation websites. Users can freely switch between the two coordinated views via the Settings Panel (Figure 4), with in-between animated transitions that communicate the two views' visual relationships (Figure 2).

2.2.1 Summary View. To convey the overall reliability of the target website, the Summary View (Figure 1A) provides a *summary statement* (e.g., "**22 misinformation websites** are mentioning **thegatewaypundit.com**") and a *doughnut chart* that represents the distributions of the sites linked with the target site. As misinformation sites often mention

[1] https://developer.twitter.com/en/docs/twitter-api/v1/tweets/search/guides/standard-operators
[2] https://github.com/IUNetSci/botometer-python

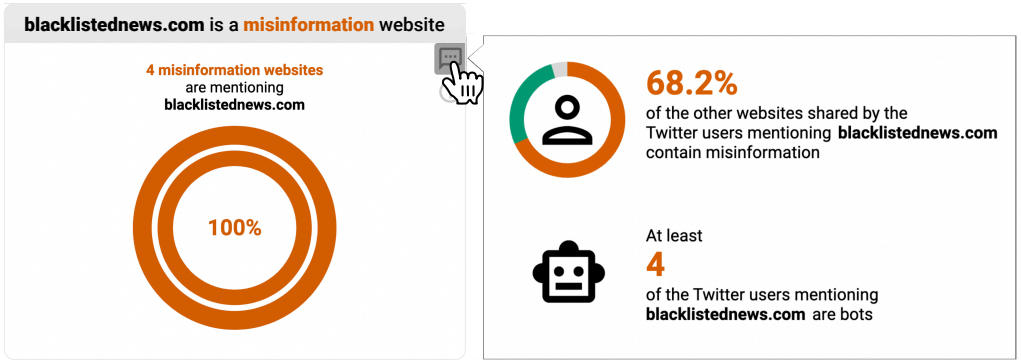

Fig. 3. When a user clicks social media button of MisVis, Twitter User Window is shown, to inform the user of two key characteristics of the Twitter users that have shared information from the target website (e.g., blacklistednews.com [1, 20]): (1) the reliability distributions of the sites shared by those Twitter users; and (2) the number of bot accounts that have mentioned the target website.

other misinformation sites (e.g., using other sites' articles as "supporting evidence") [30], the summary statement raises the user's awareness about the target site's risk by highlighting the number of misinformation sites that are mentioning it—the large number of mentioning sites is a telltale sign that the target site is indeed spreading misinformation [14].

Below the summary statement, MisVis displays a doughnut chart consisting of two rings. The inner ring represents the target site's 1-hop neighbors, and the outer ring the 2-hop neighbors. The 2-hop neighborhood provides rich information for understanding misinformation connections [14, 28]. For each site's reliability, we use its original label provided by Sehgal et al. [28], i.e., a site is labeled as either *misinformation* in orange, *reliable* in green, or *unlabeled* in gray. The unlabeled category is for *content aggregator* websites (e.g., *google.com*) that are known to curate a wide spectrum of content (e.g., for reuse), and for websites whose labels are not yet available. In the center of the doughnut charts, we show the percentage of misinformation websites among all sites represented in the doughnut chart.

The doughnut chart displays the website distribution in either *normalized* (the default, as shown in Figure 1A) or *absolute* mode (Figure 2, leftmost), configurable via the Settings Panel (Figure 4). In the *normalized* mode, a ring represents 100% of the sites, e.g., if 5 out of 10 sites in the inner ring are misinformation sites, then half of the inner ring (i.e., 50%) is colored orange. In the *absolute* mode, each ring is divided into 100 even arc segments, each representing one site, e.g., 5 misinformation sites is represented by 5 orange arc segments. We experimented with going beyond 100 segments and decided against it because they became illegible. If there are more than 100 sites in a ring, we display a pop-up message to inform the user that the limit has been reached, and revert to the default normalized mode.

2.2.2 Graph View. The Graph View (Figure 1B) shows the connection details and potential flow of misinformation by visualizing how a site is linked to other misinformation websites. Different from the Summary View, the Graph View represents each website as an individual node and visualize the connections between sites as edges. Matching the overall visual semantics of the Summary View, the Graph View also consists of two rings, softly outlined in gray to help users focus their attention on the individual sites and connections. A directed edge connects two sites (nodes) that are hyperlinked; the edge originates from the site that contains the hyperlink tag (i.e., `<a href="...">..</a>`), and the edge's arrow head ends at the destination site. When the user hovers the mouse cursor over a site, MisVis displays the site's domain name and highlights all of its edges.

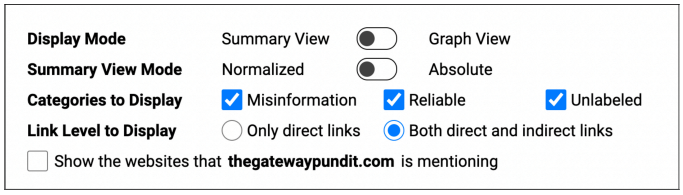

Fig. 4. The *Settings Panel* allows users to switch between Summary View and Graph View, choose the display mode for the graph in Summary View between normalized ratio and unnormalized absolute number, choose which categories of websites to display, choose whether to display indirect 2-hop websites, and choose whether to display the websites mentioned by the target site (e.g., thegatewaypundit.com).

2.3 Twitter User Window

As misinformation is commonly shared and propagated on social media [14, 30, 31], MisVis provides a complementary **Twitter User Window** (Figure 3) to inform the user of two key characteristics of the Twitter users that have shared information from the target website (e.g., blacklistednews.com [1, 20]): (1) the reliability distributions of the sites shared by those Twitter users — a high percentage of shared misinformation sites would mean that the Twitter users are "prolific" spreaders of misinformation [14, 30] and the target site is commonly shared by those users; and (2) the number of bot Twitter accounts that have mentioned the target website — a high number of bots would strongly imply that the site is misinformational as bot Twitter accounts are commonly deployed to spread misinformation [16]. The Twitter User Window is a pop-up that displays when the user click the social media button at the top-right corner of the Main Window.

2.4 Settings Panel

Users can configure the Summary View and the Graph View via the Settings Panel (Figure 4) to

- switch between the two views (described in Section 2.2);
- switch between *normalized* and *absolute* representation in Summary View (described in Section 2.2.1);
- toggle the visibility of *misinformation*, *reliable*, and *unlabeled* sites;
- toggle the visibility of the outer ring (2-hop sites); and
- choose whether to show the sites mentioned by the target website.

By default, we display all the sites within 2 hops of the target website (i.e., "both direct and indirect links" selected), as a 2-hop neighborhood provides rich information for understanding misinformation connections [14, 28]. Also by default, we do not display the sites mentioned by the target website, as it is easy for a misinformation site to deliberately link to large number of reputable sites to create a false sense of legitimacy to mislead the users.

3 USAGE SCENARIO

We present two usage scenarios where MisVis assists in understanding web misinformation connections, and informing users when surfing the web.

3.1 Exploring Connectivity of Misinformation Websites

Lisa, a graduate student studying how fake news spreads on the Internet, wants to understand how such websites are connected. She has recently seen the news that *thegatewaypundit.com* has been demonetized by Google for broadcasting

misinformation [8, 24], so she decides to learn more about the site. Lisa launches MisVis and sets *thegatewaypundit.com* as the target website. Lisa is first presented with the Summary View (Figure 1A) and learns that 14 out of the 16 sites (87.5%) directly mentioning *thegatewaypundit.com* have been labeled as misinformation, shown in orange in the inner ring. Moreover, all the websites that are 2 hops away from *thegatewaypundit.com* are also labeled as misinformation (in the outer ring). Lisa has learned from prior research that misinformation sites often mention other misinformation sites (e.g., using other sites' articles as "supporting evidence") [30]; thus, the large number of mentioning sites is a telltale sign, and Lisa is now certain that *thegatewaypundit.com* is indeed spreading misinformation [14].

Wishing to learn more about how the involved sites are connected, Lisa enters the Graph View (Figure 1B), which displays all the connections among those sites. Among all the sites, one with a particularly high degree catches Lisa's attention — *bitchute.com*, in the inner ring. Hovering over the site highlights all of its connections to other sites, helping Lisa recognize that it connects to nearly all the sites in the outer ring. This discovery helps Lisa form the hypothesis that "hub" websites with high degrees of hyperlinks (e.g., *bitchute.com*) may play important roles in spreading fake news. Thus, Lisa decides to focus her future research on understanding the connections among such misinformation websites.

3.2 A User Encountering Misinformation Website during Internet Surfing

Eric likes to browse social media for news as he likes its speed; mainstream media, in comparison, feels slow and "censored." Through a viral tweet, Eric learns about *blacklistednews.com*, which seems to be publishing a lot of niche news articles, and that excites Eric. Before spending more time on the site, he decides to use MisVis to learn about the site's reliability. To his surprise, MisVis has labeled the site as misinformation (Figure 3) [1, 20]. However, Eric is not convinced, as some news seems credible. Being an avid social media consumer, he wonders what Twitter users may think of the site, so he clicks the social media button, and the Twitter User Window pops up. Eric is astonished to learn that 68.2% of the websites mentioned by the Twitter users who have shared information from *blacklistednews.com* are misinformation sites. Eric knows that such a high percentage of shared misinformation sites means that those Twitter users are "prolific" spreaders of misinformation [14, 30] and *blacklistednews.com* is likely commonly shared by those users. Furthermore, Eric also sees that at least four bot Twitter accounts have been sharing *blacklistednews.com*, which strongly implicates the site as bot Twitter accounts are commonly deployed to spread misinformation [16]. With these important findings, Eric decides to abandon the sites, and begin his quest for more credible new sources.

4 ONGOING WORK

4.1 Human Evaluation

We plan to conduct two user studies to evaluate how MisVis may help people assess misinformation websites. The participants for the user studies will be primarily general Internet users. We plan to deploy MisVis in Docker container instances hosted on Amazon Web Services to provide a uniform secure environment for the participants to try MisVis.

The first user study aims to compare MisVis with the existing techniques that primarily alert users of misinformation. For example, for a misinformation website, we will develop two experimental conditions, where in one condition, the participants will only be presented with a "warning" message about a site (generated by existing techniques); and in the MisVis condition, the participants will be provided with MisVis to learn more about the site. The participants will be asked to rate whether the approach that they have used is informative, easy to understand, and helpful for them to assess the reliability of the site. Our goal is to understand how the visual explanations provided by MisVis may improve user's ability to assess misinformation websites.

In the second study, we will provide the participants with a list of websites, which includes both misinformation and reliable sites. The participants will be asked to access each website in the list; for each site, we will ask the participants to determine whether it is reliable. Then, we will ask the participants to learn more about the site by using MisVis, and then revisit their earlier reliability determinations — whether they remain the same or would be revised. After all the websites are accessed, we will ask the participants a series of questions that will help us quantitatively examine the impacts and effects of MisVis. Our questions, inspired by the user study in Jahanbakhsh et al. [18], will include:

- How was the information provided by MisVis helpful in assessing the reliability of the sites visited?
- How did MisVis's visualizations (e.g., Graph View) contribute to the reliability determination?
- What is the confidence in the determinations?

An exit questionnaire will ask the participants to rate MisVis's usability, and the participants' likelihood of using MisVis in the future, or recommending it to their friends. We plan to enhance MisVis with the ability to log user interactions, to help us better gain insights into the detailed usage of MisVis, such as the time they spend on each feature and the sequences in which they use those features.

4.2 Collect User Feedback for Unlabeled and Mislabeled Data

In the current domain dataset, there are websites that are not yet labeled. Also, it is not uncommon for websites to be mislabeled, as determining whether a website is misinformational can sometimes be subjective. We plan to enhance MisVis so that users may easily provide feedback for missing or wrong labels. Such feedback would help expedite the labelling process and enhance the usefulness of MisVis.

4.3 Detailed Reasoning for the Content on Misinformation Websites

MisVis focuses on how each website is shared by the other websites and social media, but currently does not consider website content. We plan to extend MisVis's explanation capability to support precisely highlighting the responsible content on site, which could be an effective way to help users make more informed determinations [11].

4.4 Deploy as Web Browser Extension

In collaboration with researchers at a large security company, we plan to deploy MisVis as a web browser extension for broader impact and improved usability. For example, as a browser extension, MisVis can automatically set its target website as the user visits it. We plan to continue to support the current usage where the user can freely enter any website as the target domain to explore it. Also, we are going to open-source MisVis for better accessibility.

5 CONCLUSION

We present MisVis, a web-based interactive tool that helps users better assess misinformation websites and understand their connections with other misinformation sites through visual explanations and novel interactive visual design. We are working to improve MisVis by adding more functions. We will evaluate the effectiveness of MisVis through user studies and deploy MisVis as a web browser extension.

REFERENCES

[1] 2017. *OpenSources.* https://github.com/OpenSourcesGroup/opensources
[2] 2022. *FAIR.* fair.org
[3] 2022. *PolitiFact.* https://www.politifact.com

[4] 2022. *Snopes.* www.snopes.com

[5] Hunt Allcott, Matthew Gentzkow, and Chuan Yu. 2019. Trends in the diffusion of misinformation on social media. *Research & Politics* 6, 2 (2019), 2053168019848554. https://doi.org/10.1177/2053168019848554

[6] Michael Bostock, Vadim Ogievetsky, and Jeffrey Heer. 2011. D^3: Data-Driven Documents. *IEEE Transactions on Visualization and Computer Graphics* 17, 12 (2011), 2301–2309. https://doi.org/10.1109/TVCG.2011.185

[7] Brett Bourbon and Renita Murimi. 2021. The Gossip Economy of Online Social Media. In *Workshop on Opinions, Intentions, Freedom of Expression, ..., and Other Human Aspects of Misinformation Online.*

[8] Abram Brown. 2021. *Google Cuts Off Ad Money To 'Gateway Pundit,' A Haven For Vaccine And Election Misinformation.* https://www.forbes.com/sites/abrambrown/2021/09/10/google-cuts-off-ad-money-to-gateway-pundit-a-haven-for-vaccine-and-election-misinformation/

[9] Giovanni Luca Ciampaglia, Prashant Shiralkar, Luis M. Rocha, Johan Bollen, Filippo Menczer, and Alessandro Flammini. 2015. Computational Fact Checking from Knowledge Networks. *PLOS ONE* 10, 6 (06 2015), 1–13. https://doi.org/10.1371/journal.pone.0128193

[10] David A Eccles and Tilman Dingler. 2021. Three prophylactic interventions to counter fake news on social media. In *Workshop on Technologies to Support Critical Thinking in an Age of Misinformation.*

[11] Rob Ennals, Beth Trushkowsky, and John Mark Agosta. 2010. Highlighting disputed claims on the web. In *Proceedings of the 19th International Conference on World Wide Web, WWW 2010, Raleigh, North Carolina, USA, April 26-30, 2010.* ACM, 341–350. https://doi.org/10.1145/1772690.1772726

[12] Lindsay Grace and Bob Hone. 2019. 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.* 1–8.

[13] Lisa Neal Gualtieri. 2009. The doctor as the second opinion and the internet as the first. In *CHI'09 Extended Abstracts on Human Factors in Computing Systems.* 2489–2498.

[14] Hans W. A. Hanley, Deepak Kumar, and Zakir Durumeric. 2022. No Calm in The Storm: Investigating QAnon Website Relationships. *ICWSM* (2022).

[15] Drahomira Herrmannova, Gautam Thakur, Joshua N. Grant, Varisara Tansakul, Bryan Eaton, Olivera Kotevska, Jordan Burdette, Martin Smyth, and Monica Smith. 2021. Challenges in Automated Detection of COVID-19 Misinformation. In *Workshop on Opinions, Intentions, Freedom of Expression, ..., and Other Human Aspects of Misinformation Online.*

[16] McKenzie Himelein-Wachowiak, Salvatore Giorgi, Amanda Devoto, Muhammad Rahman, Lyle Ungar, H Andrew Schwartz, David H Epstein, Lorenzo Leggio, and Brenda Curtis. 2021. Bots and Misinformation Spread on Social Media: Implications for COVID-19. *Journal of Medical Internet Research* 23 (2021), 5: e26933. https://doi.org/10.2196/26933

[17] Bot Sentinel Inc. 2022. *Bot Sentinel.* https://botsentinel.com

[18] Farnaz Jahanbakhsh, Amy X. Zhang, Adam J. Berinsky, Gordon Pennycook, David G. Rand, and David R. Karger. 2021. Exploring Lightweight Interventions at Posting Time to Reduce the Sharing of Misinformation on Social Media. *Proc. ACM Hum. Comput. Interact.* 5, CSCW1 (2021), 1–42. https://doi.org/10.1145/3449092

[19] Anna Kata. 2012. Anti-vaccine activists, Web 2.0, and the postmodern paradigm–an overview of tactics and tropes used online by the anti-vaccination movement. *Vaccine* 30(25) (2012), 3378–3789. https://doi.org/10.1016/j.vaccine.2011.11.112

[20] Madison Malone Kircher. 2016. *An Extremely Helpful List of Fake and Misleading News Sites to Watch Out For.* https://nymag.com/intelligencer/2016/11/fake-facebook-news-sites-to-avoid.html

[21] Ava Lew. 2021. The Unanticipated Use of Platforms in Disseminating Misinformation. In *Workshop on Opinions, Intentions, Freedom of Expression, ..., and Other Human Aspects of Misinformation Online.*

[22] Delia Mocanu, Luca Rossi, Qian Zhang, Márton Karsai, and Walter Quattrociocchi. 2015. Collective attention in the age of (mis)information. *Comput. Hum. Behav.* 51 (2015), 1198–1204. https://doi.org/10.1016/j.chb.2015.01.024

[23] Mark Craft Nabanita De, Anant Goel and Qinglin Chen. 2022. *Project Fib.* projectfib.azurewebsites.net

[24] Carly Novell. 2021. *Google finally boots Gateway Pundit from its ad platform.* https://www.dailydot.com/debug/gateway-pundit-google/

[25] Annenberg Public Policy Center of the University of Pennsylvania. 2022. *FactCheck.org.* www.factcheck.org

[26] Andrew Perrin. 2015. *Social media usage: 2005-2015.* https://www.pewresearch.org/internet/2015/10/08/social-networking-usage-2005-2015/

[27] Md Mahbub Hossain Samia Tasnim and Hoimonty Mazumder. 2020. Impact of Rumors and Misinformation on COVID-19 in Social Media. *Journal of Preventive Medicine & Public Health* 53 (2020), 171–174. https://doi.org/10.3961/jpmph.20.094

[28] Vibhor Sehgal, Ankit Peshin, Sadia Afroz, and Hany Farid. 2021. Mutual Hyperlinking Among Misinformation Peddlers. *arXiv preprint arXiv:2104.11694* (2021).

[29] Chengcheng Shao, Giovanni Luca Ciampaglia, Alessandro Flammini, and Filippo Menczer. 2016. Hoaxy: A Platform for Tracking Online Misinformation. In *Proceedings of the 25th International Conference Companion on World Wide Web (WWW '16 Companion).* International World Wide Web Conferences Steering Committee, 745–750. https://doi.org/10.1145/2872518.2890098

[30] Kate Starbird, Ahmer Arif, Tom Wilson, Katherine Van Koevering, Katya Yefimova, and Daniel Scarnecchia. 2018. Ecosystem or echo-system? exploring content sharing across alternative media domains. In *Proceedings of the International AAAI Conference on Web and Social Media*, Vol. 12.

[31] Kate Starbird, Dharma Dailey, Owla Mohamed, Gina Lee, and Emma S Spiro. 2018. Engage early, correct more: How journalists participate in false rumors online during crisis events. In *Proceedings of the 2018 CHI conference on human factors in computing systems.* 1–12.