# Editorial

# Technological Methods Against Disinformation

Leith H. Campbell

Managing Editor

**Abstract**: This editorial introduces the September issue and highlights four papers that are concerned with automatically detecting fake news and "phishing" attempts. The discussion is in the context of a recent proposal by the Australian Government to restrict the spread of misinformation and disinformation. It is noted that all the proposed methods use Artificial Intelligence (AI), suggesting that bias, which can be introduced by AI training processes, would be worthy of further research. The other papers are briefly described.

This issue also includes an obituary for Harry Wragge, a former head of Telecom/Telstra Research Laboratories. We also note the passing of John Burke, an influential member of this *Journal*'s Editorial Advisory Board.

**Keywords**: Editorial, Fake news, AI methods

## Approaches to Disinformation

Every week, it seems, we have more news about "phishing" scams, privacy breaches and the malicious spreading of misinformation and disinformation through social media. Fear and uncertainty, in some demographics at least, is holding back the further spread of the digital economy. Application developers and platform providers will find it increasingly more difficult and complex to assure users that their privacy and security are not at risk.

The "regulation" of disinformation and criminality on the Internet has, for decades, been largely in the hands of the big technology companies, particularly Google, Microsoft and Apple, together with the specialized anti-virus providers. Their methods, while widely known, at least in outline, in the tech. community, have not been subject to more general scrutiny.

Given the widespread concern about privacy and security, governments have started to introduce more formal regulation. The European Union's General Data Protection Regulation,

introduced from 2016, with amendments in 2018, has had a fundamental impact worldwide on the processing and storage of customer data and the underlying processes of websites. Now, other governments are considering more detailed regulation of content.

In June 2023, the Australian Government issued an exposure draft of proposed new legislation, the *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023*. It would give the Australian Communications and Media Authority (ACMA) powers to act "if industry efforts in regard to misinformation and disinformation are inadequate". It would enable the ACMA to request that the industry "develop a code of practice covering measures to combat misinformation and disinformation on digital platforms", with the threat that the ACMA could "create and enforce an industry standard (a stronger form of regulation), should a code of practice be deemed ineffective" (Australian Government, 2023a). This approach is similar to the one taken for the issue of news dissemination on digital platforms (Wilding, 2021).

The Government was careful to say that "private" communications, including closed chat groups, would not be covered by the legislation, and that the ACMA would not have the power to demand public content be removed. However, the proposed legislation has excited debate on whether or not it goes too far in restricting freedom of speech. The submissions to the public consultation have been available since 22 September 2023 (Australian Government, 2023b). The concerns of the Australian Human Rights Commission (Finlay, 2023) are typical: the "broad definitions [of misinformation and disinformation] used here risk enabling unpopular or controversial opinions or beliefs to be subjectively labelled as misinformation or disinformation, and censored as a result". Other submissions suggest that trust in government, generally, is low.

The Minister, in her public statements, has put some emphasis on better record-keeping and more effective systems and processes adopted by digital platforms (Minister for Communications, 2023). It is worthwhile to ask how well automated systems will perform in identifying disinformation and fake news. While the systems used by the large digital platforms are proprietary, there is now further academic interest in researching and extending the underlying technology.

In this issue, we publish four papers on the general topic of automatically identifying disinformation or phishing attempts: *Building a Fortress Against Fake News* (Fahad *et al.,* 2023); *Language-Independent Models for COVID-19 Fake News Detection* (Wong *et al.,* 2023); *Phishing Message Detection Based on Keyword Matching* (Tham, Ng & Haw, 2023); and *Improving Phishing Email Detection Using the Hybrid Machine Learning Approach* (Palanichamy & Murti, 2023). These papers offer some insight into suitable methods for

detecting disinformation and how well they could be expected to perform. The performance results should be taken as indicative only, given that proprietary systems, developed over many years through several cycles of development, are likely to perform better.

It should be noted that these systems to a greater or lesser extent all depend on Artificial Intelligence (AI) methods. While some uses of AI may turn out to be problematic, this is the benign end of the subject: a collection of data analysis procedures, some predating the "AI" tag, that help to identify features of interest in large datasets. They are now just part of the arsenal of techniques available to researchers. Like all AI, they usually come with no guarantees of providing the best possible solutions; nor should one dismiss the possibility of inherent bias, identified in other applications (Lima, Pisker & Corrêa, 2023), introduced in the "training" of the system. Bias in such systems, given that social and political prejudices may play a part in judgments about what is disinformation, would be a worthy and important topic of further research.

## John Burke

It is with sadness that we note the passing of John Burke, who was a member of the Editorial Advisory Board from the time of the *Journal*'s reformation in 2013. His initiative to found and lead what became TelSoc's Broadband Futures Group, based on discussions in the Advisory Board, was of prime importance in supporting and enhancing the *Journal*. A total of 17 related papers have been published since 2019, providing a firm fact base for TelSoc's discussions and advocacy on the need for universal broadband access.

A full obituary for John Burke will be published in a later issue.

## Elsewhere in This Issue

In addition to the four papers mentioned above, this issue contains seven other papers on a wide variety of topics.

In the Digital Economy section, we publish three papers. *Proposal of a Measurement Scale and Test of the Impacts on Purchase and Revisit Intention* looks at how to measure the effectiveness of marketing on websites. *ICT-driven Transparency: Empirical Evidence from Selected Asian Countries* provides some good news on how the use of ICT can improved transparency of governments. *Blockchain Technology for Tourism Post COVID-19* proposes some ways of improving the systems for social restrictions and travel in light of experience from the COVID-19 pandemic.

In the Telecommunications section, there are seven papers in total, the first four of which are concerned with fake news and phishing detection. Of the others, the first two, by the same

authors, *Big Data Analytics in Tracking COVID-19 Spread Utilizing Google Location Data* and *Utilizing Mobility Tracking to identify Hotspots for Contagious Disease Spread*, describe how to use Google location data to assist in tracking disease spread. The final paper, *Customer Churn Prediction through Attribute Selection Analysis and Support Vector Machine*, explores improved ways for identifying customers in danger of churning away, an important issue for telecommunications and other companies.

In the Biography section, we publish an obituary of Harry Wragge, a former head of Telecom/Telstra Research Laboratories and an influential engineer in shaping the standards and technologies underpinning Australia's telecommunications networks.

As always, we encourage you to consider submitting articles to the *Journal* and we welcome comments and suggestions on which topics or special issues would be of interest. Feedback on the current issue would be welcome.

## References

Australian Government. (2023a). Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023—Fact sheet. Department of Infrastructure, Transport, Regional Development, Communications and the Arts, June 2023. Available at https://www.infrastructure.gov.au/sites/default/files/documents/communications-legislation-amendment-combatting-misinformation-and-disinformation-bill-2023-factsheet-june2023.pdf

Australian Government. (2023b). New ACMA powers to combat misinformation and disinformation. Department of Infrastructure, Transport, Regional Development, Communications and the Arts, September 2023. Available at https://www.infrastructure.gov.au/have-your-say/new-acma-powers-combat-misinformation-and-disinformation

Fahad, N., Goh, K. O. M., Hossen, M. I., Tee, C., & Ali, M. A. (2023). Building a Fortress Against Fake News: Harnessing the Power of Subfields in Artificial Intelligence. *Journal of Telecommunications and the Digital Economy*, *11*(3), 68–83. https://doi.org/10.18080/jtde.v11n3.765

Finlay, L. (2023). Why Misinformation Bill risks Freedoms it Aims to Protect. Australian Human Rights Commission. Available at https://humanrights.gov.au/about/news/opinions/why-misinformation-bill-risks-freedoms-it-aims-protect

Lima, R. M. de, Pisker, B., & Corrêa, V. S. (2023). Gender Bias in Artificial Intelligence: A Systematic Review of the Literature. *Journal of Telecommunications and the Digital Economy*, *11*(2), 8–30. https://doi.org/10.18080/jtde.v11n2.690

Minister for Communications. (2023). Interview with Andy Park, ABC RN Drive. Transcript available at https://minister.infrastructure.gov.au/rowland/interview/interview-andy-park-abc-rn-drive

Palanichamy, N., & Murti, Y. S. (2023). Improving Phishing Email Detection Using the Hybrid Machine Learning Approach. *Journal of Telecommunications and the Digital Economy*, *11*(3), 120–142. https://doi.org/10.18080/jtde.v11n3.778

Tham, K.-T., Ng, K.-W., & Haw, S.-C. (2023). Phishing Message Detection Based on Keyword Matching. *Journal of Telecommunications and the Digital Economy*, *11*(3), 105–119. https://doi.org/10.18080/jtde.v11n3.776

Wilding, D. (2021). Regulating News and Disinformation on Digital Platforms: Self-Regulation or Prevarication? *Journal of Telecommunications and the Digital Economy*, *9*(2), 11–46. https://doi.org/10.18080/jtde.v9n2.415

Wong, W. K., Juwono, F. H., Chew, I. M., & Lease, B. A. (2023). Language Independent Models for COVID-19 Fake News Detection: Black Box versus White Box Models. *Journal of Telecommunications and the Digital Economy*, *11*(3), 84–104. https://doi.org/10.18080/jtde.v11n3.789