Introduction to the Special Issue: Re-Imagining a More Trustworthy Social Media Future

Kevin Koidl and Kristina G. Kapanova

Keywords
social media, social network, trust

Social media plays an integral role in modern society. Recently, trust-related issues have emerged related to users believing that social media platforms are misusing private information for the commercial and political benefit (Ceron, 2015). Yet, recent revelations, such as the use of information to influence democratic elections, known as the Cambridge Analytica scandal, point to the complex relationship between social media companies and users. This relationship makes it difficult to understand to what extent social media platforms influence users and the larger public (Curran & Hesmondhalgh, 2019). Moreover, social media providers tend to push the responsibility away leading to an even more distorted picture related to responsibility and accountability (Carlo Bertot et al., 2012). Contrary to the belief of mass exodus by users from social media platforms, instead users either augment their habits, or their trust in the platforms fluctuates (Turcotte et al., 2015). Such situations demonstrate the need for new approaches to data privacy and user understanding about algorithms and how they influence information propagation.

Today, social media influences almost every facet of modern life—from personal communication to dating and professional settings, we rely on social media to stay connected, to share minutiae details of our lives, to stay informed about the news (Gottfried & Shearer, 2016), to find collaborators and clients. On the other hand, such large-scale diffusion into daily routines requires an increased understanding of the risks and consequences for individuals concerning data that are wilfully shared online in a variety of platforms and situations. For instance, recent studies have focused on the role of social media in amplifying fake news propagation (Allcott & Gentzkow, 2017), hate speech (Mondal et al., 2017), and its impact on influencing political debates such as BREXIT (Del Vicario et al., 2017) and the 2016 US Presidential election (Howard et al., 2018). The revelation related to Facebook providing unfettered access to personal information about over 87 million users to Cambridge Analytica (Isaak & Hanna, 2018) has fueled the debate over not only the societal impact of those technologies but also about user’s privacy and their data rights.

Unsurprisingly, the topic of trust has come to the forefront in the debates about social media’s role in society. The opinion of users that platforms will not intentionally abuse their private information has been tested with the aforementioned Cambridge Analytica scandal, pointing to the complex nature of the relationship between social media companies and users. Conventional wisdom, once the Cambridge Analytica data breach came to light, dictated an expectancy of a mass exodus from the platforms by users, yet instead the articles in this issue show how users augment their habits toward usage but continue to participate in the platforms nonetheless (Koidl et al., 2018). Moreover, the research points out the fluctuating levels of trust in platforms depending on the situations and the news of new data breaches. Despite all the negative news and data mishandling, most users feel the social connection provided by the platforms is indispensable, especially if geographical distance is important impediment to real-life human meetings, or in relation to social status or feeling of missing out or being left out of social gatherings, thereby making it impossible to quit social media. Yet, the cognitive dissonance in users’ feelings about social media usage demonstrates the need for new approaches to data privacy and users’ understanding about algorithms and how they influence information propagation.

This Special Issue seeks to stimulate novel research focused on the relationship between social media platforms and how users can interact with them and with one another in a more trustworthy way. The far-reaching societal consequences of social media require an understanding into users’ habits, fears, and the trade-off they are willing to bear.
between the platform’s social advantages and personal privacy. In addition, the Special Issue features articles focusing on the need for new approaches to data privacy based on collective rights. The subject of algorithmic importance in information propagation and personal ad targeting has also been raised about the need for elucidating their effects on each user and the possibility of establishing new social media infrastructures, where users are the owners of the underlying algorithms and ultimate selectors of data of interest to them.

**Privacy Issues Through the Prism of Habitual Behavior**

The first section of our Special Issue includes articles focusing on identifying and understanding how users change their behavior on social media platforms with respect to protect their privacy. We begin with the study in “Negotiating Privacy and Mobile Socializing: Chinese University Students’ Concerns and Strategies for Using Geosocial Networking Applications” by Haili Li, who examines user privacy issues, attitudes, and their actions to address those concerns as seen by Chinese users through the prism of Chinese geolocated dating apps like WeChat (most used), Momo, Tantan, Bolalu, Youjia, Paipai, and Blued. The study, similar to others in this issue, found that while users contemplate privacy issues in relation to social media usage, including information misuse, leaking of personal information (bank information, publication of private messages) and tracking, and governmental surveillance, most participants rarely take any concrete steps to address those concerns, displaying trustworthy attitude by ignoring inherent privacy risks. Furthermore, the study stipulates that approach to privacy is related to individual experiences, as well as stories about privacy abuse encountered by friends and family members. In fact, few users employed active measures to mitigate the concerns they have by curtailing their social media usage or using apps with increased caution, including reporting threats to the platforms they use. Interestingly, users separate data misuse into intentional and not—with the former including apps selling user data to third parties and the latter relating to technical vulnerabilities. The issue of government surveillance through personal data exploitation was raised by the subjects, especially to censorship and their posts being removed due to opinions expressed on sensitive topics, expressing feelings of feeling unsafe or unfree in certain aspects on those social media platforms. The study considers how the particular background of users also plays a role in their social media usage. For instance between heterosexual and homosexual participants, the latter group had an increased level of concern with the topic of information leakages, as relating to their sexuality and how this can affect their daily life. Generally, women were also more conscious of possible privacy concerns. Participants with an STEM background (information technology and Internet security) were more knowledgeable about privacy issues and how to mitigate certain aspects. More often than not, instead of quitting the platforms, users decided to adjust their behavior by employing specific strategies such as being more aware of the terms of services of those platforms (which they have rarely done previously), changing the default privacy settings on the apps, considering the security consequences when location services are enabled, and most importantly the need to establish a level of trust between two users before more personal information, including pictures, is shared. A conclusion is that while users are aware of the privacy concerns, they retain a high level of trust toward the apps, opting instead to change their behavior to mitigate emerging privacy concerns.

Similar conclusions were reached in the “‘Should I Stay or Should I Leave?’: Exploring (Dis)continued Facebook Use After the Cambridge Analytica Scandal” where the author explores through in-depth interviews with undergraduate students in the United States their decision to continue or not using the social media platform and what are the factors influencing the decision, including the issue of privacy. The research depicts that the majority of interviewed participants were unsurprised by the revelations of data misuse in the case of Cambridge Analytica, although some were surprised by the ease of access to these data by third parties. The majority of the participants remained on the platform post-Cambridge Analytica scandal, with their view of Facebook remaining unchanged. Some continued their Facebook usage because they think of themselves as low engagement users, which for them is mitigation strategy for privacy issues, or holding the belief that due to the small footprint they have generated, they are not affected by data breaches. One of the main factors for remaining in Facebook was the benefit and convenience Facebook provides to staying connected, which for users outweighs any data privacy concerns they might have, illuminating the powerful network and lock-in effects Facebook enjoys as a platform. A leading psychological factor in remaining on the platform is the fear of missing out or being left out of social gatherings. Finally, if deactivated, cascading effects include the inability to use third-party services for commenting or authentication purposes.

If the first two studies engaged with users from China or United States, the third—“The Habitual Disclosure: Routine, Affordance and the Ethics of Young People’s Social Media Data Surveillance”—looks at Australian users. Southerton and Taylor explore through interviews and photo-elicitation study the level of comfort in social media platforms despite violations of privacy. Important behavioral conditioning is exemplified about people understanding social media posting not only as pleasurable and benign activity but also a necessary one due to fear of missing out or due to pressure to feel socially in good standing. As such a continuous breach of data and trust by platforms is revisited by users and made ordinary due to the daily conditioning and feeling of necessity to post by users. Despite users feeling uncomfortable by the amount of information Facebook and third-parties amass.
on them, the embeddedness of social networks in daily life precludes users from quitting due to fear of not participating, or not meeting expectations by social peers.

The fourth study—“Cybervetting and the Public Life of Social Media Data” by Gruzd et al.—examines social media about job vetting and job applicants’ trust level about this practice. Two different cultural attitudes are traced—from United States and India to understand a user’s comfort level with cyber vetting. A notable difference in privacy considerations stems from inherent differences in the culture of both countries. For instance, people from India were more comfortable with potential employers vetting their social media posting behavior, while the opposite was true for US job seekers. Importantly, when users are faced with specific privacy concerns, instead of a general all-encompassing “privacy issue,” their attitudes toward cyber vetting changes.

The described studies point out that any new privacy policies or laws about data ownership and ethics need to consider the habitual nature of social media usage.

The Role of Opinion Leaders in Information Dissemination Online

The next two articles consider the role of opinion leaders and the trust of users in them in the situation of information propagation. In “Who to Trust on Social Media: How Opinion Leaders and Seekers Avoid Misinformation and Echo Chambers,” Dubois et al. identify how despite low trust levels of users in social media platforms, the opposite might be true for opinion leaders, consequently turning the latter into a powerful information hub. Similarly, the study establishes that although people might be generally distrustful of social media algorithms, they have a higher level of trust in opinion leaders and the information their propagate, disregarding the fact that those leaders are boosted by the same algorithms, users are distrustful of.

An important function of trustworthy actors is found in “Antisemitism on Twitter: Collective Efficacy and the Role of Community Organisations in Challenging Online Hate Speech” where those agents have a positive association with larger and longer survival of information flow and ability to inhibit hateful activity. Ozalp et al. show in the case of antisemitic tweets that Jewish organizations considered trustworthy are able to see their messages propagate further and for longer periods than antagonistic messages.

In the context of trust, Deley and Dubois in “Assessing Trust vs Reliance” argue about the inherent difference between trust in people and trust in technology (e.g., Facebook and the Cambridge Analytica). A systematic review carried out in this article looks at trustworthy behavior prediction traits and the error rates of those metrics.

New Strategies Toward Data Privacy

The next articles go beyond current approaches to data privacy and protections and consider contemporary approaches, which reflect the new realities in our social media understandings.

In “Thinking Outside the Black-Box: The Case for ‘Algorithmic Sovereignty’ in Social Media,” Reviglio and Agosti focus on the algorithms that underlie our social media platforms, proposing the concept of algorithmic sovereignty. The new approach aims to give users the ability to make decisions about and control of the algorithms of data personalization. The authors proposed two types of algorithmic sovereignty: weak and strong. The former is negotiated between social media platforms and states, while the latter makes individual people the owners of the algorithms. The realization of strong sovereignty depends on the presence of algorithmic literacy—of people understanding how personalization and algorithms work and what are the particular design choices of the algorithms. Additional requirement involves the need for platforms to supply users with all the necessary data for their sovereign algorithms to personalize, based on choices made by the users themselves. Furthermore, the authors argue that social media platforms should disclose publicly the user engagement experiments they are running with users as study participants.

Finally, Lewis and Moorkens argue in “A Shared Data Ownership Approach to Trustworthy AI in Social Media” about the need for a new approach based on collective rights to the governance of AI and of the Big Data processing that drives it. The article examines current approaches to AI governance and trustworthiness, focusing on individual rights and argue that such an individualistic approach is incapable of inserting social pressure to drive change in AI and Data governance. They offer two use cases illuminating a shared data governance approach, which can give more power for negotiating with corporations and provide people with more safeguards than the current company self-regulation.

The Special Issue finalizes with the study on the study of positive influence in a prosocial activity in online groups concerning the online game Fortnite. The authors focus on the link between word choices and the intentions and behaviors of users in a game environment and conclude that prosocial acts have positive impact on the number of positive words used in the community while also showcasing that there is limited linguistic change in the negative emotion markers despite increase of prosocial behavior and positive emotions.

Concluding Remarks

Social media and with it the connected research field of social networks will remain a focus of modern society especially in relation to how social media platforms influence and shape inter-human relationships and interactions. This Special Issue points to several research projects that focus on analyzing and understanding aspects related to trust which has grown to be one of the main aspects of concern within social media. Trust not only related the platforms themselves but also related to how social media is used in general by the
individual users. Addressing aspects of trust, in recent years, several new platforms have emerged that seek to make the interaction between users more trustworthy. Examples are the Diaspora Project (diasporafoundation.org) and mastodon.social. In addition, funding and government agencies have identified the need for more trustworthy social network applications. On example is the HELIOS project (helios-social.eu) stemming from discussions within the wider research community (Koidl, 2018). In conclusion, this Special Issue has the goal to spark and promote a wider debate about trustworthy and social media bot in research and in the wider societal debate.

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) disclosed receipt of the following financial support for the research, authorship and/or publication of this article: This work is supported by the HELIOS H2020 project under grant agreement No 825585 and the ADAPT Centre, funded under the Science Foundation Ireland Research Centres Programme (Grant 13/RC/2106).

References
Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. Journal of Economic Perspectives, 31(2), 211–236.
Carlo Bertot, J., Jaeger, P., & Grimes, J. (2012). Promoting transparency and accountability through ICTs, social media, and collaborative e-government. Transforming Government: People, Process and Policy, 6(1), 78–91. https://doi.org/10.1108/1750616211214831
Ceron, A. (2015). Internet, news, and political trust: The difference between social media and online media outlets. Journal of Computer-Mediated Communication, 20(5), 487–503. https://doi.org/10.1111/jcc4.12129
Curran, J., & Hesmondhalgh, D. (2019). Media and society. Bloomsbury Academic.

Del Vicario, M., Zollo, F., Caldarelli, G., Scala, A., & Quattrociocchi, W. (2017). Mapping social dynamics on Facebook: The Brexit debate. Social Networks, 50, 6–16.
Gottfried, J., & Shearer, E. (2016). News use across social media platforms 2016. Pew Research Center. http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/
Howard, P. N., Kollanyi, B., Bradshaw, S., & Neudert, L.-M. (2018). Social media, news and political information during the US election: Was polarizing content concentrated in swing states? arXiv preprint arXiv:1802.03573.
Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. Computer, 51(8), 56–59.
Koidl, K. (2018). Towards trust-based decentralized Ad-Hoc social networks [Conference session]. Companion Proceedings of the Web Conference 2018 (WWW ‘18). International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland (pp. 1545–1551). https://doi.org/10.1145/3184558.3191608
Koidl, K., Conlan, O., Reijers, W., Farrell, M., & Hoover, M. (2018, July 18–20). The BigFoot initiative: An investigation of digital footprint awareness in social media [Conference session]. Proceedings of the 9th International Conference on Social Media and Society, Copenhagen, Denmark.
Mondal, M., Silva, L. A., & Benevenuto, F. (2017, July 4–7). A measurement study of hate speech in social media [Conference session]. Proceedings of the 28th ACM Conference on Hypertext and Social Media, Prague, Czech Republic.
Turcotte, J., York, C., Irving, J., Scholl, R. M., & Pingree, R. J. (2015). News recommendations from social media opinion leaders: Effects on media trust and information seeking. Journal of Computer-Mediated Communication, 20(5), 520–535.

Author Biographies
Kevin Koidl is a research fellow at Trinity College Dublin. His research interests are social technologies, machine learning, and natural language processing.
Kristina G. Kapanova is currently a research fellow at Trinity College Dublin. Her research interests include high-performance computing, artificial neural networks, optimization, network analysis, and social networks.