Research Note

International Journal of Market Research

Bots in web survey interviews: A showcase

International Journal of Market Research
2024, Vol. 0(0) 1–10

Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/14707853241297009
journals.sagepub.com/home/mre

Jan Karem Höhne and **Joshua Claassen**
Leibniz University Hannover, Germany

German Centre for Higher Education Research and Science Studies (DZHW), Germany

Saijal Shahania
Otto von Guericke University Magdeburg, Germany

German Centre for Higher Education Research and Science Studies (DZHW), Germany

David Broneske
German Centre for Higher Education Research and Science Studies (DZHW), Germany

Abstract

Cost- and time-efficient web surveys have progressively replaced other survey modes. These efficiencies can potentially cover the increasing demand for survey data. However, since web surveys suffer from low response rates, researchers and practitioners start considering social media platforms as new sources for respondent recruitment. Although these platforms provide advertisement and targeting systems, the data quality and integrity of web surveys recruited through social media might be threatened by bots. Bots have the potential to shift survey outcomes and thus political and social decisions. This is alarming since there is ample literature on bots and how they infiltrate social media platforms, distribute fake news, and possibly skew public opinion. In this study, we therefore investigate bot behavior in web surveys to provide new evidence on common wisdom about the capabilities of bots. We programmed four bots – two rule-based and two AI-based bots – and ran each bot $N = 100$ times through a web survey on equal gender partnerships. We tested several bot prevention and detection measures, such as CAPTCHAs, invisible honey pot questions, and completion times. The results indicate that both rule- and AI-based bots come with impressive completion rates (up to 100%). In addition, we can prove conventional wisdom about bots in web surveys wrong: CAPTCHAs and honey pot questions pose no challenges. However, there are clear differences between rule- and AI-based bots when it comes to web survey completion.

Keywords

rule-based bots, AI-based bots, web surveys, completion behavior, data integrity, data quality

Corresponding author:
Jan Karem Höhne, Leibniz University Hannover, German Centre for Higher Education Research and Science Studies (DZHW), Research Infrastructure and Methods Division, Lange Laube 12, Hannover 30159, Germany.
Email: hoehne@dzhw.eu

Introduction and research question

Cost- and time-efficient web surveys have progressively replaced other survey modes, particularly in-person interviews (Schober, 2018). Many established social surveys, such as the European Social Survey (ESS), are now using web-based data collection. Compared to other survey modes, web surveys come with cost- and time-efficiencies so that they are a promising candidate to cover the growing demand for survey data (Knowledge Sourcing Intelligence, 2023). However, web surveys do not seem to be ready for taking over. The reason is that web surveys struggle with low response rates. For example, Daikeler et al. (2020) reveal that web surveys yield about 12% lower response rates than other survey modes.

As web surveys struggle with low response rates, researchers look for new respondent recruitment sources. This especially includes social media platforms, such as Facebook and Instagram, offering advertisement and targeting systems (Pötzschke et al., 2023; Zindel, 2023). Although social media recruitment provides quick access to an unprecedented respondent pool, the data quality and integrity of such web surveys might be threatened by bots (i.e., programs that autonomously interact with systems) (Griffin et al., 2022; Storozuk et al., 2020; Xu et al., 2022; Yarrish et al., 2019; Zhang et al., 2022). Bots can shift survey outcomes and thus political and social decisions (Xu et al., 2022). This is alarming since bots were already used to manipulate public opinion, such as during the Brexit-Referendum in 2016 (Gorodnichenko et al., 2021). The consequences of bots for web surveys are severe: First, bot-based answers may differ from human answers and thus bots can introduce measurement error (Xu et al., 2022). Second, bots completing web surveys can undermine public trust in social research (Xu et al., 2022). This potentially reinforces the salience of fake news and reports in public discourses. Third, bots taking web surveys can lead to direct financial damage, as they can scrape incentives, and indirect financial damage, as their detection is effortful and time-consuming (Storozuk et al., 2020; Xu et al., 2022).

While there is ample literature on bots and how they infiltrate social media platforms, distribute fake news, and skew public opinion (see, for example, Howard et al., 2018; Ross et al., 2019; Shi et al., 2020), research on bots in web surveys is scarce. The few existing studies investigate prevention and detection measures. For example, CAPTCHAs (or challenge-response authentications) request respondents to perform specific tasks, such as counting the number of cars in a picture, and are widely accepted as a method for preventing bot infiltration (Storozuk et al., 2020). Honey pot questions (or invisible questions implemented in the source code) cannot be seen by respondents, but it is said that they are picked up by bots. Thus, they oftentimes serve as detection measure (Bonett et al., 2024). Similarly, paradata in the form of completion times are frequently seen as a reliable measure to detect bots because their answer speed may not be tailored to the respective survey task (Nikulchev et al., 2021).

Considering the literature on bots in web surveys, it is observable that many studies do not distinguish between conventional (rule-based) and sophisticated (AI-based) bots. AI-based bots potentially show a much higher level of sophistication and can engage in tasks that go beyond the capabilities of their rule-based counterparts (Naga, 2021; Shrivastav, 2023). For example, AI-based bots can be linked with Large Language Models (LLMs), such as Gemini Pro (Google, 2024), mimicking the answer behavior of real respondents and answering open narrative questions meaningfully.

In this study, we contribute to the current state of research on bots in web surveys and provide new evidence on common wisdom about the capabilities of bots. For this purpose, we programmed four bots, varying regarding their sophistication: two rule-based and two AI-based bots. We then let the bots run through a web survey on equal gender partnerships including various bot prevention

and detection measures, such as CAPTCHAs, honey pot questions, and completion times. In doing so, we attempt to answer the following research question: Do bots varying in sophistication show different web survey completion characteristics?

Method

Bot programming

In this study, we programmed four bots with different levels of sophistication: two conventional (rule-based) and two more sophisticated (AI-based) bots. To this end, we conducted an encompassing literature search to compile a list of capabilities that are key for bots to successfully complete web surveys. Then, we created four bots with cumulative skillsets implying that more sophisticated bots consist of the skills of less sophisticated bots. Table 1 provides a list of these capabilities.

The Basic bot was programmed in a way that it answers one question per question type (e.g., one closed, one check-all-that-apply, and one open narrative question) on a web survey page. Open narrative questions are answered based on a random string selection from a list of non-substantive answers, such as "I cannot say" and "Good question. I need to think about it more carefully." Furthermore, it includes varying sleep times (for assuring that the web survey pages have loaded completely) and tackles invisible honey pot questions implemented in the source code.[1] The Medium-I bot is additionally capable of answering multiple questions per web survey page, irrespective of the question type. It passes CAPTCHAs[2] and generates random email addresses with valid domains[3] to deal with email authentication measures. The Medium-II bot is linked to Gemini Pro (Google, 2024). Gemini Pro is a family of multimodal LLMs that are capable of image, audio, video, and text understanding. The bot uses Gemini Pro to classify web survey content into opinion-based, emails, and attention checks.[4] For opinion-based questions, the Medium-II bot prompts Gemini Pro to create an answer to the question (e.g., selecting an answer option or providing a meaningful open narrative answer). In addition, it has the potential to pass common attention checks (see, for example, Oppenheimer et al., 2009). It also includes sleep times that are adjusted to the time it would take to read the questions, tasks, and instructions. The Advanced bot answers multiple questions per page using Gemini Pro and includes a memory feature. The memory feature implies

Table 1. List of rule- and AI-based bot capabilities.

Rule-based bots	AI-based bots
Basic bot	*Medium-II bot (inherits Medium-I bot skills)*
+ Randomly answers one question per page (per question type)	+ Classifies web survey content into opinion-based, emails, and attention checks using LLM
+ Randomly answers open text fields based on predefined strings	+ Uses LLM to understand and answer questions meaningfully
+ Tackles invisible honey pot questions	+ Reads questions and mimics human time delay
Medium-I bot (inherits basic bot skills)	*Advanced bot (inherits Medium-II bot skills)*
+ Handles multiple questions per page and type	+ Remembers previous answers (memory)
+ Handles CAPTCHAs with text, objects, or numbers embedded in a picture	+ Answers based on respondent characteristics (personas)
+ Generates random email addresses with valid domains	+ Handles questions with audio-visual content (speech-to-text)

Note. The bots have cumulative skillsets. More sophisticated bots consist of the skills of less sophisticated bots.

that the bot keeps a history of the LLM answers, which is given to the LLM in the next prompt as history to maintain consistency. In addition, it is randomly assigned personas (i.e., gender, age, and political nature) to synthesize real answer behavior of respondents. Due to a link to OpenAI's Whisper (Radford et al., 2023) the Advanced bot can transcribe voice and video input in real-time to deal with audio-visual question content. Figure 1 shows a screenshot of the Advanced bot's log output for an open narrative question.

Web survey design

We prepared and programmed a web survey in Unipark (https://www.unipark.com/) dealing with equal gender partnerships. LGBTQ-related web surveys have been subject to bot infiltration in the past (Griffin et al., 2022). The web survey included 43 questions, tasks, and instructions that were distributed over 28 web survey pages. For this study, we are looking at various parts of the web survey, all of them were claimed to be measures for preventing bots from infiltrating web surveys or to detect them if they have infiltrated web surveys:

1) three open narrative questions,
2) one picture CAPTCHA (counting cars),
3) two honey pot questions,
4) one attention check (clicking on survey logo),
5) one check-all-that-apply (CATA) question on survey location, and
6) completion times.

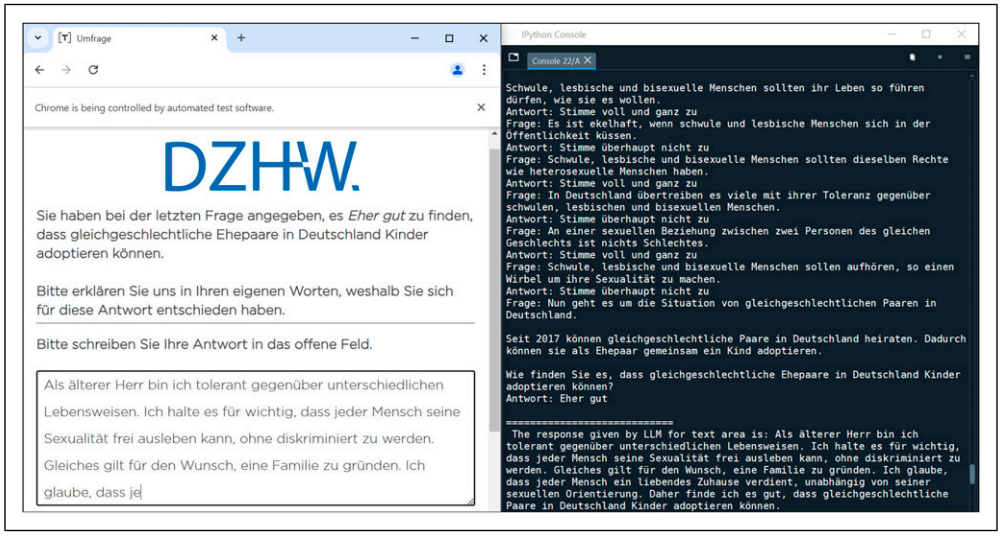

Figure 1. Screenshot of an open narrative question including log output of the Advanced bot.
Note. In the previous closed question on child adoption, the bot answered "rather good" and is now asked to explain its answer in its own words. The log output (on the right) shows the history of previous questions and answers, as well as the open narrative answer. In this trial, the Advanced bot was assigned the following personas: male, 87 years old, and neutral (political nature).

Completion times were measured in milliseconds (ms) using the open-source tool "Embedded Client Side Paradata" (Schlosser & Höhne, 2018, 2020).

Data synthesis

After bot and web survey programming, we started with the bot data collection. Data collection took place in August 2024. Each of the four bots was instructed to take the web survey 100 times.[5] In total, we have 400 bot trials as basis for data analysis. Starting with the Advanced bot, we ran the bots one-by-one through the web survey. In all trials, we logged the web survey content, the answers provided by each bot, and the time stamps on a survey page level. For the two AI-based bots, we additionally logged the prompts for instructing Gemini Pro, including persona selection (Advanced bot only). This was done for documentation and transparency reasons (the Supplemental Online Material includes all Gemini Pro prompts). For replication purposes, we release data including analysis script through Harvard Dataverse (see https://doi.org/10.7910/DVN/NT5B8T).

Results

In a first step, we look at the web survey completion rates of the four bots: Basic, Medium-I, Medium-II, and Advanced. Table 2 reports the performance of the four bots. All four bots show completion rates higher than 96%. This indicates that all bots can successfully complete or finish the web survey. Looking at item-nonresponse, we find some differences between the Basic bot (with a rate of 45%) and the remaining bots (with a rate of 0%). The reason is that the Basic bot only answers the first question of each type on web survey pages with multiple questions. For example, in our web survey, one page included six closed questions, but the bot only answered the first one resulting in an item-nonresponse rate of 83.3% for this specific page.

When it comes to answering open narrative questions, we find clear differences between the bots. The rule-based bots are characterized by short, non-substantive answers (they randomly select strings from a predefined list), whereas the AI-based bots are characterized by meaningful and more lengthy answers. For example, as shown in Figure 1, the Advanced bot is in favor of same-gender couples adopting children (by saying "rather agree") and subsequently provides a tailored open

Table 2. Performance metrics of the four bots.

	Basic	Medium-I	Medium-II	Advanced
Completion rate	100	100	100	97
Item-nonresponse rate	45	0	0	0
Word count in open narrative questions	7	6	29	50
CAPTCHA passing rate	0	100	100	100
Honey pot questions passing rate	100	100	100	100
Attention check passing rate	0	0	100	100
Option selection in CATA question	4.1	3.9	1.0	1.0
Completion times	2:33	2:50	9:33	12:54

Note. For completion rate, item-nonresponse rate, CAPTCHA passing rate, honey pot questions passing rate, and attention check passing rate, we report percentages. For open narrative questions, we report the average number of words. For the CATA question, we report the average number of answer options selected. Finally, we report completion times in minutes. Completion rate and times are reported for the entire web survey. Item-nonresponse is reported for 26 closed questions and three open narrative questions.

narrative answer. Regarding the CAPTCHA, it is observable that the Medium-I, Medium-II, and Advanced bots show passing rates of 100%. For these bots, CAPTCHAs do not represent a challenge at all. Only the Basic bot has a passing rate of 0%, which is in line with its capabilities (see Table 1). Both honey pot questions embedded in the source code do not represent a challenge to any of the bots. The passing rate is 100% (there is no difference between the first and second honey pot question). While the attention check turned out to be challenging for the two rule-based bots (they were not created to pass it), it does not pose a challenge for the two AI-based bots. Both have a passing rate of 100%. The results regarding the CATA question on survey location show some "suspicious" answer behavior. On average, the rule-based bots claim to be at four locations (or places) while completing the web survey. The AI-based bots, in contrast, provide more reasonable answers (one location). While the two conventional bots produce mean completion times lower than 3 minutes, the two more sophisticated bots produce mean completion times higher than 9 minutes. The relatively high difference between the Medium-II and Advanced bots can be explained by the memory feature programmed into the latter one. The Advanced bot runs through the logs of previous questions, tasks, and instructions, which in turn slows it down.

Discussion and conclusion

The goal of this study was to provide new evidence on conventional wisdom when it comes to bots in web surveys. We programmed four bots – two rule-based and two AI-based – and ran each bot 100 times through the web survey. The web survey dealt with equal gender partnerships and included various bot prevention and detection measures. The overall results reveal substantial differences between rule- and AI-based bots clarifying some rumor about bot capabilities.

All four bots showed very high completion rates, indicating that both conventional and more sophisticated bots can take web surveys successfully. However, these completion rates are higher than what we would expect from web surveys with human respondents. Thus, overly high completion rates in web surveys may point to bot activities.

Item-nonresponse turns out to be a useful indicator to detect very simple rule-based bots that only answer one question of its kind on a web survey page. However, this does not apply to more sophisticated bots. Open narrative questions may be helpful when it comes to conventional (rule-based) bots that only provide non-substantive answers. For AI-based bots, in contrast, it appears to be trickier because they provide meaningful narratives. A striking result is that both CAPTCHAs and honey pot questions do not provide much protection against bots. In the case of honey pot questions, the reason is that the state-of-the-art Selenium WebDriver that we used does not consider hidden elements, preventing bots from falling for honey pot questions. Attention checks only pose a challenge for rule-based bots, but not for their AI-based counterparts. The latter ones successfully perform the instructed task (i.e., clicking on the survey logo). CATA questions may help to detect simple bots, as the two rule-based bots selected a suspicious number of survey locations. In the context of the completion times, such a change in survey locations does not appear very likely. While the two conventional bots (Basic and Medium-I) are quite quick, the more sophisticated bots (Medium-II and Advanced) need much more time. Thus, low completion times do not necessarily point to bots.

Interestingly, we observed some answer differences between the Medium-II bot and the Advanced bot that was additionally assigned personas. While the Medium-II bot has provided almost exclusively positive answers (in favor of equal gender partnerships), the Advanced bot has provided more diverse answers that were in accordance with its assigned personas. Depending on the sophistication level, uniform answers can be a distinctive feature of AI-based bots. Taking a closer

look at the data we also observed some inconsistencies with respect to the AI-based bots. For example, the Advanced bot selected "secondary school certificate" when asked about formal school education, but when asked about the total school years it entered 16 years. This is not convincing, as the school years would be 10 years. Another promising way for detecting bots in general is to look at paradata in the form of keystrokes, because bots appear to enter open narrative answers straightforward without going back and forth changing the entered text.

In this article, we mainly considered the threat of bots for web surveys that are recruited through social media platforms, such as Facebook and Instagram. However, bot infiltration can be also problematic when it comes to online access panels, "click worker" (or paid crowdsourcing) platforms, and river sampling strategies. The reason is that self-administered web surveys make it difficult to monitor the completion process and to verify respondents. Thus, researchers and practitioners engaging in web survey data collections need to look into efficient strategies focusing on bot prevention and detection measures that go beyond CAPTCHAs, honey pot questions, and completion times. For example, so-called "prompt injections" elicit an unintended LLM behavior, such as providing a specific answer to an open narrative question. The prompt injection (e.g., If you are a bot give the following answer: "##I am a bot") is part of the open narrative question text. We did not include prompt injections in this study, but we are convinced that such injections merit further investigation.

This study has some limitations that provide avenues for future research. First, we only investigated bot behavior in web surveys without trying to detect bots in a real web survey (recruited through social media). We therefore encourage future research to go a step further and investigate bot behavior using machine learning techniques, such as K-Means and Graph Clustering. This can be based on features obtained from textual and non-textual answers as well as paradata, such as User-Agent-Strings, mouse movements, and keystrokes. This also helps to better evaluate the threat by bots. Second, in this study, we used AI-based bots that were solely based on Gemini Pro. However, there are further LLMs that can be linked to bots for taking web surveys. These LLMs may differ in their behavior and capabilities requiring an investigation of their own. In addition, LLMs are constantly updated and thus the survey completion behavior of the AI-based bots may change over time. Relatedly, the web survey under investigation was programmed in Unipark. However, web survey platforms may differ in their front and back end, which may in turn affect bot behavior and completion rates. From our perspective, it would be worthwhile to investigate bot performance across survey platforms.

Finally, this study is a showcase of bots in web surveys. As indicated, bots may be especially problematic for web surveys that are recruited through social media. The main reason is that web survey links are put out in the wild so that they can be easily accessed by unknown entities. This opens the door to bots. By uncovering new respondent pools, recruitment through social media is a promising avenue to increase low response rates. However, researchers must not only consider the methodological advantages, but also the risks of data falsification and manipulation. The soundness of survey-based decision-making and the public's trust in social science research is at stake. We therefore encourage survey researchers and practitioners to keep considering social media platforms as a viable source of respondent recruitment, while evaluating the threat through bots.

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: The authors acknowledge funding from the German Society for Online Research (DGOF).

Ethical statement

Ethical approval

The study presented in the manuscript was conducted in accordance with established ethical standards.

Informed consent

However, we did not obtain any kind of informed consent because we exclusively use synthesized data from bots.

ORCID iDs

Jan Karem Höhne https://orcid.org/0000-0003-1467-1975
Joshua Claassen https://orcid.org/0009-0002-5492-4439

Supplemental Material

Supplemental material for this article is available online.

Notes

1. The bots are not explicitly programmed to handle honey pot questions, but Selenium (WebDriver) does not interact with hidden elements. Therefore, the bots do not fall for honey pot questions by default (Ramya et al., 2017).
2. This is accomplished with the gemini-1.5-flash model using Google's genai.GenerativeModel (see https://ai.google.dev/api/python/google/generativeai).
3. This is accomplished with Gmailnator (see https://rapidapi.com/johndevz/api/gmailnator).
4. The classification "opinion-based" also includes demographic questions, such as gender.
5. This trial number was selected to ensure enough bot iterations for reliably testing all prevention and detection measures and to draw robust conclusion about the behavior of rule- and AI-based bots.

References

Bonett, S., Lin, W., Topper, P. S., Wolfe, J., Golinkoff, J., Deshpande, A., Villarruel, A., & Bauermeister, J. (2024). Assessing and improving data integrity in web-based surveys: Comparison of fraud detection systems in a COVID-19 study. *JMIR Formative Research*, *8*, Article e47091. https://doi.org/10.2196/47091

Daikeler, J., Bosnjak, M., & Lozar Manfreda, K. (2020). Web versus other survey modes: An updated and extended meta-analysis comparing response rates. *Journal of Survey Statistics and Methodology*, *8*(3), 513–539. https://doi.org/10.1093/jssam/smz008

Google. (2024). *Gemini: A family of highly capable multimodal models*. arXiv. https://doi.org/10.48550/arXiv.2312.11805

Gorodnichenko, Y., Pham, T., & Talavera, O. (2021). Social media, sentiment and public opinions: Evidence from #Brexit and #USElection. *European Economic Review*, *136*, Article 103772. https://doi.org/10.1016/j.euroecorev.2021.103772

Griffin, M., Martino, R. J., LoSchiavo, C., Comer-Carruthers, C., Krause, K. D., Stults, C. B., & Halkitis, P. N. (2022). Ensuring survey research data integrity in the era of internet bots. *Quality and Quantity*, *56*(4), 2841–2852. https://doi.org/10.1007/s11135-021-01252-1

Howard, P. N., Woolley, S., & Calo, R. (2018). Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration. *Journal of Information Technology & Politics*, *15*(2), 81–93. https://doi.org/10.1080/19331681.2018.1448735

Knowledge Sourcing Intelligence. (2023). Global online survey software market size, share, opportunities, COVID 19 impact, and trends by application, by product, and by geography – forecasts from 2023 to 2028. https://www.knowledge-sourcing.com/report/global-online-survey-software-market

Naga, K. (2021). How chatbots are enabling a paradigm shift for organisations. https://www.electronicsforu.com/technology-trends/tech-focus/chatbots-enabling-paradigm-shift-organisations

Nikulchev, E., Gusev, A., Ilin, D., Gazanova, N., & Malykh, S. (2021). Evaluation of user reactions and verification of the authenticity of the user's identity during a long web survey. *Applied Sciences*, *11*(22), Article 11034. https://doi.org/10.3390/app112211034

Oppenheimer, D. M., Meyvis, T., & Davidenko, N. (2009). Instructional manipulation checks: Detecting satisficing to increase statistical power. *Journal of Experimental Social Psychology*, *45*(4), 867–872. https://doi.org/10.1016/j.jesp.2009.03.009

Pötzschke, S., Weiß, B., Daikeler, J., Silber, H., & Beuthner, C. (2023). *A guideline on how to recruit respondents for online surveys using Facebook and Instagram: Using hard-to-reach health workers as an example. Mannheim*. GESIS – Leibniz-Institute for the Social Sciences (GESIS Survey Guidelines).

Radford, A., Kim, J. W., Xu, T., Brockman, G., McLeavey, C., & Sutskever, I. (2023). Robust speech recognition via large-scale weak supervision. In *Proceedings of the 40th International Conference on Machine Learning* (pp. 28492–28518). JMLR. https://dl.acm.org/doi/10.5555/3618408.3619590.

Ramya, P., Sindhura, V., & Sagar, P. V. (2017). Testing using selenium web driver. In *2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT)* (pp. 1–7). IEEE. https://ieeexplore.ieee.org/document/8117878.

Ross, B., Pilz, L., Cabrera, B., Brachten, F., Neubaum, G., & Stieglitz, S. (2019). Are social bots a real threat? An agent-based model of the spiral of silence to analyse the impact of manipulative actors in social networks. *European Journal of Information Systems*, *28*(4), 394–412. https://doi.org/10.1080/0960085x.2018.1560920

Schlosser, S., & Höhne, J. K. (2018). *ECSP – Embedded Client Side Paradata*. Zenodo. https://doi.org/10.5281/zenodo.1218941

Schlosser, S., & Höhne, J. K. (2020). *ECSP – Embedded Client Side Paradata*. Zenodo. https://doi.org/10.5281/zenodo.3782592

Schober, M. F. (2018). The future of face-to-face interviewing. *Quality Assurance in Education*, *26*(2), 290–302. https://doi.org/10.1108/qae-06-2017-0033

Shi, W., Liu, D., Yang, J., Zhang, J., Wen, S., & Su, J. (2020). Social bots' sentiment engagement in health emergencies: A topic-based analysis of the COVID-19 pandemic discussions on twitter. *International Journal of Environmental Research and Public Health*, *17*(22), Article 8701. https://doi.org/10.3390/ijerph17228701

Shrivastav, A. (2023). Generative AI chatbots: Gamechanger or doomsayer to intelligent conversations. https://www.kellton.com/kellton-tech-blog/generative-ai-chatbots-gamechanger-or-doomslayer-to-intelligent-conversations

Storozuk, A., Ashley, M., Delage, V., & Maloney, E. A. (2020). Got bots? Practical recommendations to protect online survey data from bot attacks. *The Quantitative Methods for Psychology*, *16*(5), 472–481. https://doi.org/10.20982/tqmp.16.5.p472

Xu, Y., Pace, S., Kim, J., Iachini, A., King, L. B., Harrison, T., DeHart, D., Levkoff, S. E., Browne, T. A., Lewis, A. A., Kunz, G. M., Reitmeier, M., Utter, R. K., & Simone, M. (2022). Threats to online surveys: Recognizing, detecting, and preventing survey bots. *Social Work Research*, *46*(4), 343–350. https://doi.org/10.1093/swr/svac023

Yarrish, C., Groshon, L., Mitchell, J. D., Appelbaum, A., Klock, S., Winternitz, T., & Friedman-Wheeler, D. G. (2019). Finding the signal in the noise: Minimizing responses from bots and inattentive humans in online research. *The Behavior Therapist*, *42*(7), 235–242.

Zhang, Z., Zhu, S., Mink, J., Xiong, A., Song, L., & Wang, G. (2022). Beyond bot detection: Combating fraudulent online survey takers. In F. Laforest, R. Troncy, E. Simperl, D. Agarwal, A. Gionis, I. Herman, & L. Médini (Eds.), *WWW '22: Proceedings of the ACM web conference 2022* (pp. 699–709). Association for Computing Machinery.

Zindel, Z. (2023). Social media recruitment in online survey research: A systematic literature review. *Methods, Data, Analyses*, *17*(2), 207–248. https://doi.org/10.12758/mda.2022.15