2020 ■ Vol. 16 ■ no. 5

Got Bots?
Practical Recommendations to Protect Online Survey Data from Bot Attacks

Andie Storozuk [a], Marilyn Ashley [a], Véronic Delage [a] & Erin A. Maloney [a]

[a]University of Ottawa, School of Psychology

Abstract ■ The Internet has been a popular source of data amongst academic researchers for many years, and for good reason. Online data collection is fast, provides access to hard-to-reach populations, and is often less expensive than in-lab recruitment. With these benefits also come risks, such as duplicate responses or participant inattention, which can significantly reduce data quality. Very recently, researchers have become aware of another concern associated with online data collection. Bots, also known as automatic survey-takers or fraudsters, have begun infiltrating scientific surveys, largely threatening the integrity of academic research conducted online. The aim of this paper is to warn researchers of the threat posed by bots and to highlight practical strategies that can be used to detect and prevent these bots. We first discuss strategies recommended in the literature that we implemented to identify bot responses from online survey data we collected in the past six months. We then share which strategies proved to be most and least effective in detecting bots. Finally, we discuss the implications of bot-generated data for the integrity of online research and the imminent future of bots in online data collection.

Keywords ■ online data collection, bots, fraudulent responses, data integrity.

Acting Editor ■ Denis Cousineau (Université d'Ottawa)

✉ erin.maloney@uottawa.ca

10.20982/tqmp.16.5.p472

Introduction

In the summer of 1991, the World Wide Web was made publicly available, forever altering the way researchers recruit participants and gather data. Since its inception, researchers have commended the utility of the Internet for scientific purposes (e.g. Kelley-Milburn & Milburn, 1995; McGlade, Milot, & Scales, 1996). The Internet presents a unique set of advantages as a methodological tool, such as prompt data collection, access to hard-to-reach populations, and low costs in comparison to in-lab studies (Alessi & Martin, 2010; Hash & Spencer, 2009; Wright, 2005). There are, however, disadvantages to online data collection, and we are undoubtedly not the first to address these pitfalls (e.g. Reips, 2002; Stanton, 1998; Whitehead, 2007). Such concerns include: (a) duplicate responses that may be unintentional or for profit (Kramer et al., 2014; Reips, 2002; Teitcher et al., 2015); (b) careless responding or insufficient effort responding to survey items (Huang, Curran, Keeney, Poposki, & DeShon, 2012; Meade & Craig, 2012); (c) identity fraud (i.e., lying about demographic information to meet eligibility criteria; Chandler & Paolacci, 2017); and (d) inability to control the survey environment (Zwarun & Hall, 2014). These issues with online data collection pose serious threats to data quality and validity, increasing potential for Type I and Type II errors (Credé, 2010; Huang, Liu, & Bowling, 2015; McGonagle, Huang, & Walsh, 2016; McGrath, Mitchell, Kim, & Hough, 2010; Woods, 2006).

Despite these methodological concerns, the Internet remains a common source of scientific data and researchers continuously place trust in technology within their methodological frameworks. However, as scientists innovate and technology continues to advance, we must ask ourselves, are we taking advantage of technology, or is technology taking advantage of us? In addition to the existing concerns of data collected online, researchers are facing a new online threat – bots. Bots are malicious software applications programmed to complete automated tasks online, such as filling out surveys, to receive compensation (Dupuis, Meier, & Cuneo, 2019; Teitcher et al., 2015). In

the literature, bots have also been referred to as automatic survey-takers (Godinho, Schell, & Cunningham, 2020), automated form-fillers (Buchanan & Scofield, 2018, 6), botnets (Dupuis et al., 2019), and fraudsters (Teitcher et al., 2015). For the remainder of this paper, we will use the term bot as an umbrella term to refer to these fake, automated participants.

Bots pose a serious threat to the integrity of scientific data, as bot-generated data is completely invalid (Dupuis et al., 2019). Programmed to complete surveys much faster than human participants, bots can complete the same survey repeatedly (Teitcher et al., 2015). If not caught quickly, bots can overwhelm researchers with hundreds of fraudulent responses in a matter of hours. Worse still, researchers that financially compensate participants may be extorted for thousands of dollars, paying bot programmers for invalid, unusable data. But researchers are not entirely culpable for being deceived by bots; over the years, bots have become progressively more difficult to discern from human participants. Posing as legitimate users, bot profiles appear increasingly credible and intelligible. This is especially true for automated accounts known as "cyborgs" or "sock puppets," profiles that are carefully monitored by human programmers to ensure their bots' responses are coherent and realistic (Samuels & Akhtar, 2019).

are we taking advantage of technology, or is technology taking advantage of us?

Only gaining serious attention in the past five years, the prevalence of bot-generated data in academic research is unknown as it has not yet been formally estimated (Dupuis et al., 2019; Shanahan, 2018). Researchers suspect that bot activity is on the rise, however, given the growing number of commercially available bots (Dupuis et al., 2019; Shanahan, 2018) and the ease with which bots can be obtained and programmed (Buchanan & Scofield, 2018, 6). Imperva's Threat Research Lab provides a yearly comprehensive overview of bot activity on all Internet websites. According to the latest report, only 62.8% of all Internet traffic in 2019 could be attributed to human users, meaning that 37.2% of Internet traffic was bots (Imperva, 2020). Alarmingly, the proportion of "bad bots" (i.e., bots designed to engage in criminal activity) relative to "good bots" (i.e., bots designed to help users navigate web pages) is growing, accounting for 24.1% of bot traffic in the year 2019 (Imperva, 2020).

The conversation concerning bots extends beyond academic articles, reaching platforms such as blogs (e.g. Howell, n.d. LibertyM [@LibertyM], 2020; Moss & Litman, n.d. Shanahan, 2018; Simone, 2019) and Twitter (e.g. Simone, n.d.). Dr. Melissa Simone, a quantitative, social, and developmental psychologist, shared her personal experience with bots on Twitter, warning fellow researchers that "checking the quality of [their] data every few days" will no longer suffice (Simone, n.d.). Rather, researchers need to put strategies in place to protect the veracity of online data and prevent the infiltration of bot respondents. This proactive vigilance is important to consider as the on-going COVID-19 pandemic forces many researchers to design studies with contactless methodologies. Due to the current global context, researchers who may typically collect data in-person have been unexpectedly thrust into the world of online data collection. Given the uncertainty of the prevalence of bots in scientific data, and the serious threat bots pose to data reliability and validity, it is imperative that researchers: (a) know how to protect their data from being infiltrated by bots; (b) are aware of what constitutes evidence of bots in their data; and (c) remove fraudulent responses from their data.

Purpose

Even with many academic researchers relying heavily on the Internet for data collection purposes, few have reported on the data cleaning techniques they employ to address bot responses (Dupuis et al., 2019; Godinho et al., 2020; Teitcher et al., 2015). As such, we felt it prudent to address this issue, sharing herein what we have learned through trial and error of implementing various bot-detection strategies in our own data. Below we discuss our experiences with bots from several datasets collected online in the past six months (June 2020 to present).

How Did We Know That We Had Bots?

There were several clues in our datasets to suggest that we had a bot problem. Within 24 hours of launching one of our surveys, we received 470 responses – an extremely improbable influx. Multiple responses had the exact same start and end time, which is not likely to occur by chance. Responses to open-ended questions were nonsensical, contradictory, or identical to responses from other participants. Despite eligibility requirements stating we were recruiting solely Canadian residents, many participants entered American zip codes as opposed to Canadian postal codes. We immediately halted data collection and turned to the literature for guidance on how to proceed.

What Does the Literature Recommend?

Several strategies have been suggested to try to mitigate the issue of bot respondents. In their thorough review, Teitcher et al. (2015) propose that researchers can detect and prevent Internet research fraud in four ways: (a) by

Table 1 ■ Effectiveness of Bot Detection and Prevention Strategies

Effectiveness	Strategy
Most effective	Screening email addresses
	Screening open-ended responses and reverse scored items
	Not sharing the survey link publicly
	Monitoring time of survey completion
	Monitoring speed of survey completion
Moderately effective	Embedding a CAPTCHA into the survey
	Checking the eligibility of IP addresses
	Attention check questions
Least effective	Honeypot questions
	Presenting text as an image

Note. The effectiveness of bot detection strategies is based on the proportion of bots identified in our datasets using the strategy in question.

adding elements to the online questionnaire (e.g., attention check questions or CAPTCHAs), (b) by screening the legitimacy of participants' personal data (e.g., email addresses), (c) by examining eligibility of computer information (e.g., IP addresses), and (d) by modifying the study design (e.g., require face-to-face interviews). Godinho et al. (2020) categorize these safeguards against bots as either automatized techniques (i.e., embedded in surveys, such as CAPTCHAs) or ongoing manual techniques throughout recruitment (e.g., consistent screening of emails or IP addresses). Given that comprehensive reviews on the techniques researchers can use to detect bots already exist (see Teitcher et al., 2015; Godinho et al., 2020), it is beyond the scope of this paper to reiterate how to employ these various strategies. Instead, we will discuss the strategies that we chose to implement in our own research, expand on some of these strategies, and then discuss the effectiveness of these strategies in identifying bots in our data.

What Did We Do to Try to Mediate Our Bot Issue?

There were many strategies proposed both in the literature and on online forums on how best to deal with bots in survey data. Below, we elaborate on the strategies implemented in our data and their effectiveness in detecting or deterring bot respondents (see Table 1). Note that Simone (2019) suggests flagging participants with two or more infractions as potential bots.

Most Effective Strategies

Email Addresses

We were able to detect hundreds of bots by using participants' email addresses, as recommended in Teitcher and colleagues' review (2015). When screening email addresses for indicators of bots, it is important to look for multiple email addresses in concession that have remarkably similar patterns. For example, email addresses may follow a pattern of six letters (e.g., arphbl) or may follow a pattern of first name, last name, X numbers (e.g., RobinSmyth607958) before the address sign. Another indicator, as we discovered in our data, is the use of temporary email addresses, such as YOPmail. YOPmail enables users to create temporary email addresses without registration. Although the service claims to "guard [users] against spam, phishing, and other online abuses" (YOPmail, n. d.), it puts researchers' data at risk for these exact concerns. Importantly, Teitcher et al. (2015) indicate that bots may in fact have multiple, dissimilar, and valid email addresses that would not be detected by our screening techniques. This point illustrates the necessity of using several strategies to identify the majority of bots present in datasets.

Given our (previous) ignorance to bots, we had to screen email addresses for suspicious activity after much of the data had already been collected. Godinho et al. (2020), however, suggest collecting email addresses prior to data collection so that participants must verify their identity before they are permitted to take part in the study. Though this method removes some anonymity and slows recruitment speed, the authors argue that this extra step within the recruitment process has the potential to prevent invalid data, ultimately outweighing the potential loss of participants and time (Godinho et al., 2020). Another screening option is to have potential participants sign up for the study using a Google form. In this case, interested participants will only be sent the survey link by the researcher after their email address has been pre-screened.

Open-Ended Responses and Reverse Scored Items

Advocated by Simone (2019, n.d.), the screening of open-ended questions proved to be an excellent method to de-

tect bots. For many of the bots in our data, open-ended questions were either not answered, were incomprehensible (e.g., "Curriculum resources creatively mining"), were unrelated to the question, or were exactly the same as another respondent who answered the survey in close temporal proximity. Responses that contradicted each other were also an indicator of potential bot activity. An example from our dataset revealed inconsistencies between a child's reported age and grade level. This respondent indicated that their child was seven years old, but then indicated that this same child was in grade seven. Given participants were required to be living in Canada, their child should be 12 or 13 years old if in grade seven, not seven years old.

Including items that required reverse scoring was also important in detecting inconsistencies and potential straightlining (also known as longstring or nondifferentiation). For example, a measure of trait anxiety included items that were both positive (e.g., "I am content") and negative (e.g., "I worry too much over something that really doesn't matter"), with the positive items being reverse scored and summed with the negative items, such that higher scores were indicative of higher levels of trait anxiety (Spielberger & Gorsuch, 1983). Participants that agree to positive items should correspondingly disagree with negative items. Those that do not conform to this pattern of responses show signs of inattention, insufficient effort responding, or automated responding. Bots aside, this assessment is a valuable screening tactic when evaluating the quality of data from human participants (Herzog & Bachman, 1981; Johnson, 2005; Yan, 2008).

Not Sharing the Survey Link Publicly

Though social media platforms appear to be an ideal medium to connect with potential research participants, they are also convenient for bot programmers to identify and target research studies (Simone, n.d.; Pozzar et al., 2020, 10). Twitter and Facebook are some of the main platforms bot hackers use to find research studies. Traditionally, the authenticity procedures set in place by Twitter were lacking, making it easier for programmers to automate accounts on this platform (Samuels & Akhtar, 2019). More recently, Twitter has invested heavily in the detection of fraudulent accounts by requiring email or phone number authentication, auditing existing accounts, and expanding malicious behaviour detection systems (Roth & Harvey, 2018). However, with the advancement of detection strategies comes the advancement of bot programming, as these effective strategies force bots to become smarter to remain hidden on the platform (Samuels & Akhtar, 2019).

It is not recommended to share the survey link publicly (Pozzar et al., 2020, 10). Rather, one solution we implemented was to have interested participants contact us to obtain the survey link (by using Google forms, as mentioned previously). This method reduced the number of bots but did not eliminate them, as bots still emailed us to attempt to obtain the survey link. It is simple to spot these bot emails, as the subject lines are often poorly written or nonsensical (e.g., "INTERESTING THE STUDY"). Bots may use keywords or phrases from your study advertisement in the subject line of their email (e.g., "To participate in the study, or find out more" or "Under investigation"). Bots may also use generic statements about research in the subject line (e.g., "Hello. I can participate in your research" or "I would like to participate in your online research" or "I hope I can help in your research"). Further indication that an inquiry is disingenuous is that body messages of bot spam emails are often left blank. If the email contains a body message, it typically does not include a greeting or sign-off, is nonsensical (e.g., "I like to investigate, please link me"), lacks sentence structure, and has poor grammar (e.g., "Great, I participate in survey"). By not sharing survey links publicly, researchers can significantly reduce the number of bots that gain access to their study, thus making data monitoring far more manageable.

Time of Survey Completion

We also looked at the time of day the survey was completed as a potential sign of fraudulent activity. This is not necessarily a hard indicator of a bot (it is very possible a human participant may complete a survey late at night), but it serves as a red flag to look for other bot indicators from this respondent. From our experience, bots tended to hack our survey links during the middle of the night. Thus, responses between the hours of 12 a.m. and 6 a.m. were marked as suspicious. When using this screening tactic, the researcher must take into consideration the geographic population they are targeting. If your survey is open to anyone, anywhere in the world, then time of day may not be a relevant factor. If you are limiting recruitment to a specific geographic location, then take into consideration that time zone specifically.

Speed of Survey Completion

Many features that make bots powerful, such as their fast responses and high rates of productivity, are often the same features that expose them (Shanahan, 2018). Monitoring the speed of survey completion has been recommended as a method to identify bots (Teitcher et al., 2015). The researcher must use their discretion for what they feel is an acceptable completion speed or for what constitutes a response that is "too fast." Teitcher et al. (2015) recommend a cut-off could be set to two standard deviations above or below the mean completion time. It should be

noted, however, that this tactic only proved to be useful to us early in the recruitment process. The bots gradually became more effective at hiding in the survey data by completing the study at more reasonable rates so as to not be detected.

Moderately Effective Strategies

CAPTCHA

A CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) is a type of challenge–response test used to determine whether a computer user is human. In our own data, it is difficult to determine how effective the CAPTCHA was in detecting bots, given that we are unaware of the number of bots who were unable to pass this screener and enter our survey. Though CAPTCHAs are a great first line of defense, they should not be considered a bot "catch-all," as not all CAPTCHA codes are secure. Godinho et al. (2020) warn that CAPTCHAs can be bypassed easily and should therefore be accompanied by frequent monitoring of the data. Dupuis et al. (2019) point out that bot programmers may bypass the CAPTCHA by completing it themselves before setting up their bots to finish the remainder of the survey. Nonetheless, researchers should always include a CAPTCHA at the beginning of each online survey to prevent less sophisticated bots from accessing their survey.

IP Addresses

Another strategy recommended by Teitcher et al. (2015) and Godinho et al. (2020) was to ensure that back-end paradata, such as IP addresses, match recruitment criteria. Given that our surveys were intended for Canadian residents, any IP addresses traced to a location outside of Canada could be an indication of a bot. Further, any repeated IP addresses may also be cause for concern, as this could be a sign that one respondent has completed the survey multiple times.

However, the legitimacy of using IP addresses as a screening method has been a topic of contention. Dennis, Goodson, and Pearson (2019) argue that IP addresses should not be used to identify individuals and are an insufficient means of evaluating data quality. Indeed, multiple eligible participants may complete the survey from the same IP address (e.g., same computer or from the same general location, such as a university campus; Teitcher et al., 2015). IP addresses can also be easily modified or faked to appear legitimate, preventing researchers from knowing where the participant is located and whether they have completed the survey multiple times (Teitcher et al., 2015; Dennis et al., 2019). By using virtual private networks (VPNs), participants can conceal the IP address of their devices (Dennis et al., 2019). Though the use of VPNs largely complicates a researchers' decision of whether to attribute a response to a bot or a human, participants using VPNs may not necessarily have malicious intent. For many people, the use of VPNs have become commonplace for Internet security purposes or as a method for accessing content that is restricted to certain geographic locations (e.g., obtaining an American IP address to gain access to content on Netflix). Dennis et al. (2019) also note that there is no official database that links IP addresses to locations, forcing researchers to rely on databases created by private companies. Researchers should be cautious when drawing conclusions about bots by using IP addresses and should only use this technique in tandem with multiple other strategies.

Attention Check Questions

Attention check questions, or "trap questions," can be a valuable tool to indicate an increased risk of lower data quality (**provide Liu & Wronski**; **2018 lw18**). These questions can be structured in two ways: (a) as directed questions, requiring participants to provide a specific response (Huang et al., 2012; Maniaci & Rogge, 2014; Meade & Craig, 2012); and (b) as bogus questions, requiring participants to respond to items that everyone should agree to (i.e., universal truths such as "I was born on planet Earth") or disagree to (i.e., universal falsities such as "I can teleport across time and space") (Dunn, Heggestad, Shanock, & Theilgard, 2018; Huang et al., 2015; Meade & Craig, 2012). Like many other data quality indicators, attention check questions should be examined within the context of other screening techniques. From our experience, these questions catch bots early in the recruitment process, but bots quickly learn the correct answers and become less detectable through these types of questions.

Least Effective Strategies

Honeypot Questions

Honeypots are decoy questions embedded in a survey that are programmed to engage and deceive bot respondents. Importantly, honeypots are not visible to human participants. Thus, if a respondent answers a honeypot question, then they have exposed themselves as a bot. Sophisticated bots are able to detect honeypots that stand out thematically from other items in the survey (Simone, 2019). As such, we designed our honeypots to appear plausible in relation to the content of the survey. The JavaScript code found on this Qualtrics Community post (LibertyM [@LibertyM], 2020) was used to "hide" questions from humans and lay the bait for bots. Although the honeypot questions were successfully hidden from humans, none of the

bots provided responses to these trap questions. Other researchers have reported similar findings, whereby honeypots did not receive responses (e.g. Moss & Litman, n.d.). These results may have occurred because bots have advanced beyond the scope of honeypot questions and are now too sophisticated to be exposed using this strategy. That said, researchers should still implement honeypots in online surveys, given that these hidden questions pose no extra work for human participants and may catch a few bots in the process (e.g. Pozzar et al., 2020, 10).

Text Presented as An Image

It has been suggested that bots are incapable of decoding images of distorted text (Carnegie Mellon University, n. d.), however, this has not been our experience. All bots in our data were able to decipher text instructions presented as an image or a distorted image (e.g., Figure 1). Therefore, we do not recommend this strategy to detect or deter bots.

Other Considerations – What Else Can We Do?

Provide Personal Survey Links

One way to combat the influx of bot respondents is to provide personalized, single-use survey links for each participant (Pozzar et al., 2020, 10). This will not necessarily stop bots from accessing your survey but will prevent bots from completing the survey multiple times from the same link.

Modify Compensation

We believe people should be compensated for their work. However, we suspect that financial compensation (e.g., providing Amazon.ca gift cards) attracted many bots to our studies. Although removing compensation entirely would likely deter the bots, it would also likely deter human participants. There are many benefits of compensating participants, such as increased response rates (Wright, 2005), increased completion rates, a reduction in various incomplete participation patterns (Bosnjak & Tuten, 2003), and decreases in careless responding (Bowling et al., 2016; Huang et al., 2015). However, there is evidence to suggest that data validity issues are especially prevalent when incentives are offered (Bowen, Daniel, Williams, & Baird, 2008; Konstan et al., 2005; Murray et al., 2009; Wright, 2005). For example, Chandler and Paolacci (2017) found that participants were more likely to reattempt a survey in a high-pay condition (15.8%) compared to a low-pay condition (5.7%), indicating fraud was more prevalent when compensation was higher.

To deter bots from completing a study for financial purposes, some researchers recommend conducting a lottery draw as opposed to providing individual payments (Kramer et al., 2014; Teitcher et al., 2015). However, this strategy may inadvertently attract more fraudulent responses as a way of increasing participants' chances of winning (i.e., "stacking the deck" in their favour). Wright (2005) suggests that incentives redeemable for real merchandise, such as books, may be more effective at deterring fraudulent entries. Kramer et al. (2014) recommend not advertising the amount or type of compensation that will be provided, though we speculate that this strategy may not receive Research Ethics Board approval.

Statistical Analyses

Dupuis et al. (2019) recommend using Mahalanobis distance to detect multivariate outliers and person–total correlations to determine the extent to which a set of responses fits general tendencies. According to the authors, these analyses produce high detection rates and are simple to calculate using basic statistical programs (Dupuis et al., 2019). However, in their study, Dupuis et al. (2019) compared the merit of various indicators of fraudulent data under the assumption that bots respond in a completely random pattern. Given what we know about bots, this approach is potentially problematic, as not all bot-generated responses are necessarily random. From our experience, bots learn from the survey questions and can produce increasingly intelligible responses the longer they have access to the survey. Our attention check questions, for example, were able to catch bots early in the launch of the study. Within one day, all bots were able to respond correctly to these trap questions, providing evidence that they "learned" from previous mistakes and adjusted their responses accordingly. For this reason, like the other strategies mentioned, we further stress the importance of using this detection method in conjunction with other indicators.

Lessons Learned

Bots Can Learn

As we learn about bots, they learn about us. Evidence from our data suggests that bots are capable of learning and adapting quickly (e.g., correct responses to attention check questions, slower completion speeds), making such fraudulent responses increasingly difficult to detect. The longer bots have access to a survey, the better they become at imitating human responses. As such, bot screening techniques that are currently successful may not be shrewd enough in the future. We have already seen this to be true with CAPTCHA technology and honeypot questions. Though CAPTCHAs and honeypots were highly efficient when first released, they no longer catch many of the more sophisticated bots.

Figure 1 ■ Image of the University of Ottawa Postal Code. Participants were instructed to either provide their own postal code or type the postal code presented in this image into a text box. This distorted image was created using Microsoft Paint's Airbrush function.

Recruit from A Reliable Source

The most effective way to deal with bots is to keep them out of your survey in the first place. Recruit participants from a reliable source, such as an existing database in your laboratory or department. Many researchers claim that online participant pools, such as Amazon's Mechanical Turk (MTurk), are reliable sources of data (e.g. Buhrmester, Kwang, & Gosling, 2011; Holden, Dennie, & Hicks, 2013; Johnson & Borden, 2012). Recently, such pools have been under question for the reliability of the data collected from MTurk workers (e.g. Aruguete et al., 2019; Rouse, 2015). Additionally, researchers have highlighted the concern of professional participants, or "super workers," and bots in these sample pools (Chandler, Mueller, & Paolacci, 2014; Chmielewski & Kucker, 2019; Dennis et al., 2019; Fort, Adda, & Cohen, 2011; Stewart et al., 2015). When collecting data from online resources, researchers need to be cautious and always use a trusted source of legitimate data.

Shut Down the Survey Link

The moment you notice suspicious activity in your data, shut down the survey link. Once bots have access to a link, they will rapidly -and repeatedly- respond to the survey, leaving you with hundreds of responses to sort through after only a matter of hours. If a link has been infiltrated by bots, it is best to close the contaminated link and create a new one.

Do Not Automate Compensation

Allow time to screen the data for potential bots before compensating participants. By paying bots, the validity of the study is reduced while also increasing research costs; a lose-lose situation for researchers (Dupuis et al., 2019).

Use as Many Screening Strategies as Possible

As we have discussed, it is important to use multiple screening strategies. By using multiple indicators, researchers can more accurately identify bots, reducing the number of bots that are able to evade these measures and slip between the cracks.

Discussion

Bots threaten the quality of scientific data and increase the likelihood of Type I and Type II errors. Like inattentive and deceptive humans, bots cause serious threats to the reliability and validity of study results. There is evidence to suggest that invalid data can significantly alter study results, even at rates as low as 5% (Credé, 2010). As part of the research community, we all have a responsibility to maintain data integrity, given that the reliability of research findings depends on high quality data (Buchanan & Scofield, 2018, 6). One important piece of this puzzle is to remain diligent in our practice of screening for fraudulent activity. It is imperative that we, as a community, do not provide bots the opportunity to learn. By granting bots access to a survey, they learn how to become more difficult to detect, thus perpetuating the cycle for other researchers. Similarly, as Open Science practices become more widespread, researchers are collaborating and sharing their datasets more often. Therefore, it is of best practice for researchers to deter and detect bots to guarantee the quality of studies that use the same data.

To best ensure data integrity and transparency, set up a pre-registered plan for bot data screening (Buchanan & Scofield, 2018, 6; Pozzar et al., 2020, 10). When filtering bots from the data, be sure to document which participants have been removed and for what reason. Importantly, before using the bot-detection strategies presented above, be sure to have proper ethics board clearance from your own institution. This is particularly relevant to studies that compensate each participant as one likely does not want to be compensating bots for fraudulent data.

Where Do We Go from Here?

The new, disturbing, reality is that bot-activity in survey data is inevitable. Evidence from the data we collected suggests that bots are capable of learning. Responses to open-ended questions become more comprehensible the longer the bots have access to a survey. Researchers must not become complacent or rely solely on automated screening techniques (such as CAPTCHAs) to filter out bots. Even with protections in place, the speed at which bots learn

suggests they will continue to bypass our protections. As Simone (2019) cautions, we are in an arms race with bots; "As researchers develop and deploy data protection tools, bot programmers find ways around them." To uphold a high quality of online research, we must remain vigilant in our fight against bots.

Authors' note

This research has been funded by a Natural Sciences and Engineering Research Council of Canada Development Grant to Erin A. Maloney, a Social Sciences and Humanities Research Council of Canada Insight Development Grant to Erin A. Maloney, and an Ontario Graduate Scholarship to Andie Storozuk.

References

Alessi, E. J., & Martin, J. I. (2010). Conducting an internet-based survey: Benefits, pitfalls, and lessons learned. *Social Work Research*, *34*(2), 122–128. doi:10.1093/swr/34.2.122

Aruguete, M. S., Huynh, H., Browne, B. L., Jurs, B., Flint, E., & McCutcheon, L. E. (2019). How serious is the 'carelessness' problem on mechanical turk? *International Journal of Social Research Methodology*, *22*(5), 441–449. doi:10.1080/13645579.2018.1563966

Bosnjak, M., & Tuten, T. L. (2003). Prepaid and promised incentives in web surveys: An experiment. *Social science computer review*, *21*(2), 208–217. doi:10.1177/0894439303021002006

Bowen, A. M., Daniel, C. M., Williams, M. L., & Baird, G. L. (2008). Identifying multiple submissions in internet research: Preserving data integrity. *AIDS and Behavior*, *12*(6), 964–973. doi:10.1007/s10461-007-9352-2

Bowling, N. A., Huang, J. L., Bragg, C. B., Khazon, S., Liu, M., & Blackmore, C. E. (2016). Who cares and who is careless? insufficient effort responding as a reflection of respondent personality. *Journal of Personality and Social Psychology*, *111*(2), 218–218. doi:10.1037/pspp0000085

Buchanan, E. M., & Scofield, J. E. (2018). Methods to detect low quality data and its implication for psychological research. *Behavior Research Methods*, *50*, 2586–2596. doi:10.3758/s13428-018-1035-6

Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's mechanical turk: A new source of inexpensive, yet high-quality, data? *Perspectives on Psychological Science*, *6*(1), 3–5. Retrieved from https://dx.doi.org/10.1177/1745691610393980

Carnegie Mellon University. (n. d.). Captcha: Telling humans and computers apart automatically. Retrieved November 16, 2020, from http://www.captcha.net/

Chandler, J. J., Mueller, P., & Paolacci, G. (2014). Nonnaïveté among amazon mechanical turk workers: Consequences and solutions for behavioral researchers. *Behavior research methods*, *46*(1), 112–130. doi:10.3758/s13428-013-0365-7

Chandler, J. J., & Paolacci, G. (2017). Lie for a dime: When most prescreening responses are honest but most study participants are impostors. *Social Psychological and Personality Science*, *8*(5), 500–508. doi:10.1177/1948550617698203

Chmielewski, M., & Kucker, S. (2019). An mturk crisis? shifts in data quality and the impact on study results. *Social Psychological & Personality Science*, *11*(4), 1948550619. doi:10.1177/1948550619875149

Credé, M. (2010). Random responding as a threat to the validity of effect size estimates in correlational research. *Educational and Psychological Measurement*, *70*, 596–612. doi:10.1177/0013164410366686

Dennis, S., Goodson, B., & Pearson, C. (2019). Online worker fraud and evolving threats to the integrity of mturk data: A discussion of virtual private servers and the limitations of ip-based screening procedures. *SSRN Electronic Journal*, *18*, 44–47. doi:10.2308/bria-18-044

Dunn, A. M., Heggestad, E. D., Shanock, L. R., & Theilgard, N. (2018). Intra-individual response variability as an indicator of insufficient effort responding: Comparison to other indicators and relationships with individual differences. *Journal of Business and Psychology*, *33*(1), 105–121. doi:10.1007/s10869-016-9479-0

Dupuis, M., Meier, E., & Cuneo, F. (2019). Detecting computer-generated random responding in questionnaire-based data: A comparison of seven indices. *Behav Res*, *51*, 2228–2237. doi:10.3758/s13428-018-1103-y

Fort, K., Adda, G., & Cohen, K. B. (2011). Amazon mechanical turk: Gold mine or coal mine? *Computational Linguistics*, *37*(2), 413–420. doi:10.1162/COLI_a_00057

Godinho, A., Schell, C., & Cunningham, J. A. (2020). Out damn bot, out: Recruiting real people into substance use studies on the internet. *Substance Abuse*, *41*(1), 3–5. doi:10.1080/08897077.2019.1691131

Hash, K. M., & Spencer, S. M. (2009). You've got subjects: The promise of the internet in research with lesbian. gay, bisexual and transgender populations. In W. Meezan & J. I. Martin (Eds.), *Handbook of research with gay, lesbian, bisexual, and transgender populations* (pp. 238–258). New York: Routledge.

Herzog, A. R., & Bachman, J. G. (1981). Effects of questionnaire length on response quality. *Public opinion quarterly*, *45*(4), 549–559. doi:10.1086/268687

Holden, C. J., Dennie, T., & Hicks, A. D. (2013). Assessing the reliability of the m5-120 on amazon's mechanical

turk. *Computers in Human Behavior*, *29*(4), 1749–1754. doi:10.1016/j.chb.2013.02.020

Howell, B. (n.d.). Dealing with bots, randoms and satisficing in online research. Retrieved November 16, 2020, from https://www.psychstudio.com/articles/bots-randoms-satisficing/

Huang, J. L., Curran, P. G., Keeney, J., Poposki, E. M., & DeShon, R. P. (2012). Detecting and deterring insufficient effort responding to surveys. *Journal of Business and Psychology*, *27*(1), 99–114. doi:10.1007/s10869-011-9231-8

Huang, J. L., Liu, M., & Bowling, N. A. (2015). Insufficient effort responding: Examining an insidious confound in survey data. *Journal of Applied Psychology*, *100*(3), 828–832. doi:10.1037/a0038510

Imperva. (2020). *Bad bots report*. New York: Imperva Research Labs.

Johnson, D. R., & Borden, L. A. (2012). Participants at your fingertips: Using amazon's mechanical turk to increase student–faculty collaborative research. *Teaching of Psychology*, *39*(4), 245–251. doi:10.1177/0098628312456615

Johnson, J. (2005). Ascertaining the validity of individual protocols from web-based personality inventories. *Journal of Research in Personality*, *39*(1), 103–129. Retrieved from https://dx.doi.org/10.1016/j.jrp.2004.09.009

Kelley-Milburn, D., & Milburn, M. A. (1995). Cyberpsych: Resources for psychologists on the internet. *Psychological Science*, *6*(4), 203–211. doi:10.1111/j.1467-9280.1995.tb00594.x

Konstan, J. A., Rosser, S., R., B., Ross, M. W., Stanton, J., & Edwards, W. M. (2005). The story of subject naught: A cautionary but optimistic tale of internet survey research. *Journal of Computer-Mediated Communication*, *10*(2), 0-0. doi:10.1111/j.1083-6101.2005.tb00248.x

Kramer, J., Rubin, A., Coster, W., Helmuth, E., Hermos, J., Rosenbloom, D., ... Brief, D. (2014). Strategies to address participant misrepresentation for eligibility in web-based research. *International Journal of Methods in Psychiatric Research*, *23*(1), 120–129. doi:10.1002/mpr.1415

LibertyM [@LibertyM]. (2020). Hidden question traps for bots [online forum post]. Retrieved November 16, 2020, from https://www.qualtrics.com/community/discussion/6152/hidden-question-traps-for-bots

Maniaci, M. R., & Rogge, R. D. (2014). Caring about carelessness: Participant inattention and its effects on research. *Journal of Research in Personality*, *48*, 61–83. doi:10.1016/j.jrp.2013.09.008

McGlade, L. T., Milot, B. A., & Scales, J. (1996). The world wide web: A new research and writing tool. *The American Journal of Clinical Nutrition*, *63*, 981–982.

McGonagle, A. K., Huang, J. L., & Walsh, B. M. (2016). Insufficient effort survey responding: An underappreciated problem in work and organisational health psychology research. *Applied Psychology*, *65*(2), 287–321. doi:10.1111/apps.12058

McGrath, R. E., Mitchell, M., Kim, B. H., & Hough, L. (2010). Evidence for response bias as a source of error variance in applied assessment. *Psychological bulletin*, *136*(3), 450–459. doi:10.1037/a0019216

Meade, A. W., & Craig, S. B. (2012). Identifying careless responses in survey data. *Psychological methods*, *17*(3), 437–457. doi:10.1037/a0028085

Moss, A., & Litman, L. (n.d.). After the bot scare: Understanding what's been happening with data collection on mturk and how to stop it. Retrieved November 16, 2020, from https://www.cloudresearch.com/resources/blog/after-the-bot-scare-understanding-whats-been-happening-with-data-collection-on-mturk-and-how-to-stop-it/

Murray, E., Khadjesari, Z., White, I., Kalaitzaki, E., Godfrey, C., McCambridge, J., ... Wallace, P. (2009). Methodological hallenges in online trials. *Journal of Medical Internet Research*, *11*(2), e9–, e9–11. doi:10.2196/jmir.1052

Pozzar, R., Hammer, M. J., Underhill-Blazey, M., Wright, A. A., Tulsky, J., Hong, F., ... Berry, D. L. (2020). Threats of bots and other bad actors to data quality following research participant recruitment through social media: Cross-sectional questionnaire. *Journal of Medical Internet Research*, *22*, e23021–e23021. doi:10.2196/23021

Reips, U. D. (2002). Internet-based psychological experimenting: Five dos and five don'ts. *Social science computer review*, *20*(3), 241–249. doi:10.1177/08939302020003002

Roth, Y., & Harvey, D. (2018). How twitter is fighting spam and malicious automation. Retrieved June 26, 2020, from https://blog.twitter.com/official/en_us/topics/company/2018/how-twitter-is-fighting-spam-and-malicious-automation.html

Rouse, S. V. (2015). A reliability analysis of mechanical turk data. *Computers in Human Behavior*, *43*, 304–307. doi:10.1016/j.chb.2014.11.004

Samuels, E., & Akhtar, M. (2019). Are 'bots' manipulating the conversation? here's what's changed since 2016. Retrieved November 20, 2019, from https://www.washingtonpost.com/politics/2019/11/20/are-bots-manipulating-conversation-heres-whats-changed-since/

Shanahan, T. (2018). Are you paying bots to take your online survey? Retrieved March 22, 2018, from https://www.forsmarshgroup.com/knowledge/news-blog/posts/2018/march/are-you-paying-bots-to-take-your-online-survey/

Simone, M. (n.d.). Lesson 2: Everyone doing online data collection needs to build in ***complex and advanced*** logic/inattentional checks [tweet]. Retrieved September 17, 2019, from https://twitter.com/m_simonephd/status/1174012127197257728

Simone, M. (2019). Bots started sabotaging my online research. i fought back. Retrieved November 21, 2019, from https://www.statnews.com/2019/11/21/bots-started-sabotaging-my-online-research-i-fought-back/

Spielberger, C. D., & Gorsuch, R. L. (1983). *State-trait anxiety inventory for adults: Manual and sample: Manual, instrument and scoring guide*. Raccoon City: Consulting Psychologists Press.

Stanton, J. M. (1998). An empirical assessment of data collection using the internet. *Personnel psychology*, *51*(3), 709–725. doi:10.1111/j.1744-6570.1998.tb00259.x

Stewart, N., Ungemach, C., Harris, A. J., Bartels, D. M., Newell, B. R., Paolacci, G., & Chandler, J. (2015). The average laboratory samples a population of 7,300 amazon mechanical turk workers. *Judgment and Decision making*, *10*(5), 479–491.

Teitcher, J. E., Bockting, W. O., Bauermeister, J. A., Hoefer, C. J., Miner, M. H., & Klitzman, R. L. (2015). Detecting, preventing, and responding to "fraudsters" in internet research: Ethics and tradeoffs. *The Journal of Law, Medicine & Ethics*, *43*(1), 116–133. doi:10.1111/jlme.12200

Whitehead, L. C. (2007). Methodological and ethical issues in internet-mediated research in the field of health: An integrated review of the literature. *Social science & medicine*, *65*(4), 782–791. doi:10.1016/j.socscimed.2007.03.005

Woods, C. M. (2006). Careless responding to reverse-worded items: Implications for confirmatory factor analysis. *Journal of Psychopathology and Behavioral Assessment*, *28*(3), 186–192. doi:10.1007/s10862-005-9004-7

Wright, K. B. (2005). Researching internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services. *Journal of computer-mediated communication*, *10*(3), 259–271. doi:10.1111/j.1083-6101.2005.tb00259.x

Yan, T. (2008). Nondifferentiation. In P. J. Lavrakas (Ed.), (pp. 520–521). Racoon City: Sage publication.

YOPmail. (n. d.). Disposable and free email address. Retrieved from http://www.yopmail.com/en/

Zwarun, L., & Hall, A. (2014). What's going on? age, distraction, and multitasking during online survey taking. *Computers in Human Behavior*, *41*, 236–244. doi:10.1016/j.chb.2014.09.041

Citation

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. doi:10.20982/tqmp.16.5.p472

Received: 12/11/2020 ~ Accepted: 16/11/2020