Original Article

Methodological Innovations
September-December 2021: 1–10

DOI: 10.1177/20597991211050467
journals.sagepub.com/home/mio
SAGE

Suspicious and fraudulent online survey participation: Introducing the REAL framework

Jennifer Lawlor[1], Carl Thomas[2], Andrew T Guhin[2], Kendra Kenyon[2], Matthew D Lerner[3], UCAS Consortium and Amy Drahota[2]

Abstract

Online survey research has significantly increased in popularity in recent years. With its use, researchers have a new set of concerns about data collection and analysis to consider, including the possibility of fraudulent survey submissions. The purpose of this article is to demonstrate to survey researchers an innovative and systematized process for addressing online survey fraud over the course of collecting survey data, especially when respondents collect incentives for participation. We provide the **R**eflect, **E**xpect, **A**nalyze, **L**abel Framework, which includes four sets of guiding questions for use by online survey researchers to plan for addressing survey fraud and making determinations about the inclusion or exclusion of participant submissions from the dataset based on level of suspicion. We also provide a full case example utilizing the **R**eflect, **E**xpect, **A**nalyze, **L**abel Framework as an appendix. Those wanting to apply the **R**eflect, **E**xpect, **A**nalyze, **L**abel Framework should keep in mind several considerations as they apply it, including determining logistical needs ahead of survey implementation, considering the ethical issues related to including or excluding data in a study, and considering the issues related to providing incentives for participating in research. Future research should assess the frequency of survey fraud, investigate the reasons for its occurrence and explore the role social networks may play in fraudulent participants sharing information. We suggest that researchers consider online survey fraud as an issue over the lifespan of their survey and apply the guiding questions we present to address the issue throughout.

Keywords

Online research, survey research, online survey, survey fraud

Introduction

Social Science researchers who employ online surveys are becoming increasingly aware that some participants are fraudulently gaining access to their surveys that include incentives for participation, and often are doing so multiple times. The COVID-19 pandemic has elevated this issue by moving many in-person surveys to online venues (Palamar and Acosta, 2020). Survey fraud can be uniquely challenging in online research as there are many avenues for potential "fraudsters" to access surveys, and as the landscape of the Internet has changed, so too have the avenues fraudsters use. As psychologists and other researchers frequently employ online platforms to conduct research, survey fraud can create substantial issues in the field related to data validity. There are unique approaches to prevent, discover, and exclude fraudulent responses using survey technology and data analysis techniques that researchers should consider when collecting participant data online.

In this article, we outline the **R**eflect, **E**xpect, **A**nalyze, and **L**abel (REAL) Framework, developed for researchers to

[1]School of Information, University of Michigan, Ann Arbor, MI, USA
[2]Department of Psychology, Michigan State University, East Lansing, MI, USA
[3]Department of Psychology, Stony Brook University, Stony Brook, NY, USA

Corresponding author:
Jennifer Lawlor, School of Information, University of Michigan, 105 S. State St., Ann Arbor, MI 48109, USA.
Email: jalawlor2@gmail.com

identify suspected online survey fraud, especially when respondents collect incentives for participation, and make decisions about including or excluding suspicious responses. We first provide a brief background on survey fraud and identify frameworks for addressing fraud as a gap in current knowledge. We then detail the REAL Framework for identifying online survey fraud. We conclude with future directions for applying and refining the REAL Framework.

Background

Survey fraud has been defined several ways. Some define it as participants completing multiple surveys (Teitcher et al., 2015); others as the provision of misinformation on surveys, focusing on participants that purposefully misrepresent themselves in order to receive study participation incentives (Hulland and Miller, 2018). However, in this paper, we conceptualize survey fraud and suspicion as the following:

1. *Unique Participant Fraud*. Survey fraud that involves individuals who use the same identifying information in order to access a survey multiple times. This can occur either with the intention of accepting multiple incentives or for legitimate reasons (e.g. the participant was not sure that their first survey was correctly recorded, or they simply forgot they had already participated). These are submissions where it is clear that a single individual has submitted multiple responses.
2. *Alias Fraud*. Survey fraud that includes sophisticated techniques aimed at concealing the identity of a single individual submitting multiple responses.
3. *Suspicious Submissions*. Survey submissions that could be fraudulent (unique participant fraud or alias fraud).

Survey fraud and suspicious survey submissions should be of concern to researchers as it increases the amount of random error in a dataset, possibly leading to erroneous conclusions, and can force them to seek a much larger sample than needed in order to account for the noise introduced. Although this issue can create substantial roadblocks for researchers, survey research still lacks a comprehensive framework for identifying and addressing suspicious submissions. Thus, the REAL Framework attempts to fill this gap.

Online survey research

Online survey research has substantially increased over time, providing both advantages and disadvantages in the research process. Practical advantages of online surveys and online research in general include the ability to reach global or hard-to-reach audiences, convenience for researchers and participants, low research costs relative to in-person survey administration, and ease of data entry and analysis (Evans and Mathur, 2018; Hammond, 2018; Reips, 2000; Wright, 2005; Wyatt, 2000). Participants may also provide less socially desirable responses to questions about sensitive topics due to increased privacy online (Bowen et al., 2008; Teitcher et al., 2015).

Drawbacks to online survey research include self-selection bias among participants, under-coverage of individuals without Internet access, and participants' ability to misrepresent their eligibility to participate or mask their identities in order to participate multiple times in a single study (Bethlehem, 2010; Wright, 2005). Researchers may offer incentives that increase fraudulent activity if the same individual participates multiple times or participates knowing they are ineligible. The same participant may use different email addresses to complete multiple submissions to get compensation (Wright, 2005). Conversely, choosing not to offer incentives may remove some interest among participants to submit a survey when they are ineligible or have participated once. Fraudulent submissions are common in online research, and after excluding invalid submissions, there may be a smaller sample size (Bauermeister et al., 2012). This can undermine the statistical power of the data if the researcher later must reduce the pool of responses being analyzed and can add statistical noise to the data that masks findings. To continue to reap the benefits of survey research, researchers must address the challenges that come with using online surveys.

Contemporary methods for managing fraud

Fraud management literature contains numerous methods to include in survey procedures to address fraud. These can be summarized based on when they occur in the survey process: pre-data collection, during data collection, and post-data collection. They can be further broken down into prevention-focused methods and exclusion-focused methods. We briefly summarize each of these in Table 1. No single method can completely protect against fraudulent or suspicious submissions and there is no single set of methods that works for all surveys at all times.

Pre-data collection

Pre-data collection, researchers can make prevention-focused recruitment plans targeted at specific groups. To limit information about the existence of the survey, single use or personalized links can be used in recruitment efforts (Reips, 2002a; Teitcher et al., 2015). Pre-survey screening questions can also identify whether a potential participant meets the inclusion criteria for the study (Chandler and Paolacci, 2017; Hulland and Miller, 2018; Jones et al., 2015).

While these approaches are intended to prevent fraudulent responses from becoming part of the survey data, there are

Table 1. Summary of tools for identifying suspicious survey responses.

Research phase	Preventive or exclusionary	Strategy	References
Pre-data collection	Preventive	Single use link	Reips, 2002a; Teitcher et al., 2015
		Targeted recruitment	–
		Pre-survey screening questions	Chandler and Paolacci, 2017; Hulland and Miller, 2018; Jones et al., 2015
Data collection	Preventive	CAPTCHA	Teitcher et al., 2015
		Cookies	Teitcher et al., 2015
	Exclusionary	Seriousness checks	Aust et al., 2013; Gosling et al., 2004; Mustanski, 2001; Nosek et al., 2002; Pequegnat et al., 2007
		Trick questions	Aust et al., 2013; Gosling et al., 2004; Mustanski, 2001; Nosek et al., 2002; Pequegnat et al., 2007
		Personal identifiers	Bauermeister et al., 2012; Bowen et al., 2008; Jones et al., 2015; Konstan et al., 2005; Pequegnat et al., 2007; Reips, 2002a, 2002b; Reips et al., 2015
		Survey meta data (e.g. IP address, date and time stamp, geolocation data)	Konstan et al., 2005; Muir and Van Oorschot, 2009; Mustanski, 2001; Pequegnat et al., 2007; Reips et al., 2015; Ryan, 2018; Schmidt, 1997; Teitcher et al., 2015
Post-data collection	Exclusionary	Identity verification process	See personal identifiers above
		Response patterns or meta data within and across submissions	Gosling et al., 2004; Mustanski, 2001

Note: "Preventive" refers to measures employed to inhibit fraudulent responses from being submitted, "exclusionary" refers to measures used to identify submissions that should be excluded from analysis.

many ways that individuals can work around them. Individuals wanting to take a survey without qualifying or wanting to take it multiple times can identify the correct answers to pre-screening questions in order to participate anyway by persistently taking screening questions and identifying those that will provide access to the full survey (Chandler and Paolacci, 2017). Even single use links should be monitored as participants may request additional links in order to participate more than once in the survey. Careful oversight may prevent those who have already submitted a survey from receiving a second link, but this often requires additional team resources. For example, research teams may designate a member who carefully monitors survey responses for patterns of suspicious responses in order to identify those suspected to be fraudulent.

Data collection

Researchers can also use the data collection stage to employ preventive measures. A completely automated public Turing test to tell humans and computers apart, also known as CAPTCHA question, ensures that participants are not bots. Researchers can also add questions to their survey to test the seriousness of responses, include trick questions, or instructional manipulations that make it difficult to move quickly through a survey (Aust et al., 2013; Gosling et al., 2004; Nosek et al., 2002; Oppenheimer et al., 2009; Pequegnat et al., 2007). They can also directly ask questions about participants' identities (e.g. email addresses, unique passwords, or names) or learn about participants through survey metadata (e.g. IP address, geolocation, date of submission) to pinpoint if a participant appears multiple times (Bauermeister et al., 2012; Bowen et al., 2008; Jones et al., 2015; Konstan et al., 2005; Muir and Van Oorschot, 2009; Mustanski, 2001; Pequegnat et al., 2007; Reips, 2002a, 2002b; Reips et al., 2015; Ryan, 2018; Schmidt, 1997; Teitcher et al., 2015). They can also use cookies, which put a small data packet on a computer to flag it has already been used for a submission, to prevent multiple submissions from the same computer (Teitcher et al., 2015).

Post-data collection

Collecting personal identifiers and meta data are among the most popular tools for identifying suspicious responses; however, these have unique challenges in their use. For example, participants can easily create multiple email addresses or aliases to provide if a survey asks for them. Furthermore, it has also gotten easier over time to mask meta data, like IP addresses or geolocation searches using methods like virtual private servers (Hauser et al., 2019).

Post-data collection researchers can use exclusionary approaches to identify patterns in response, metadata, and recruitment logs. Psychometric analysis can indicate whether a set of responses is consistent with previous properties for the questions being asked, and indicate the quality of responses (Gosling et al., 2004; Mustanski, 2001). Assessing

metadata and patterns between surveys can reveal patterns in multiple submissions from the same or different people based on their location, IP address, or date and time of submission. Assessing metadata within surveys (e.g. the length of time spent on each page of the survey, consistency in responses, and questions that establish seriousness) can also serve as an indicator of response quality.

Each of these approaches comes at a cost to researchers or to participants and none of them is foolproof in preventing or identifying instances of fraud. Preventive measures may increase the burden on participants who must answer unrelated survey questions in the form of screeners or seriousness checks, which can also increase fatigue. Participants that are co-located and share computers may be inconvenienced or excluded using cookies or IP addresses. In addition, asking participants to provide identifiable information reduces participant privacy and may decrease their trust in the survey or research team. After a survey has been administered, researchers must have expertise and time to identify suspicious submissions. This can require substantial time and investment in identifying and removing the problematic data. Thus, researchers must be intentional in selecting the most appropriate method for their study to identify survey fraud in order to reduce or manage the costs and maximize the benefits.

While these methods to managing fraud in the literature give us a set of tools for managing survey fraud, they do not provide a way of approaching online surveys to reduce the incidence of fraud that is adaptive to the unique circumstances of individual projects, and especially for projects that involve participant incentives. Each of the methods in the literature, when applied individually, resolve specific and often straightforward types of fraud, particularly unique participant fraud. To address more complex fraud, specifically alias fraud, an adaptive fraud management plan that can be applied across the lifespan of a survey is required. In addition, past fraud management methods have already become outdated. For example, using IP addresses to identify multiple survey responses from a single individual is now difficult because the ability for an individual to mask their IP address has improved (Hauser et al., 2019). Focusing on how to conceptualize and plan for survey fraud, rather than promoting use of discrete tools, will help to create a more robust fraud defense.

In addition, there are ethical considerations involved in determining which survey responses are suspicious enough to be excluded from analyses. Legitimately eligible participants contribute their time and experience to research. Making sure illegitimate participants are excluded from the dataset ensures that the trends in data from legitimate participants are reported as accurately as possible. These decisions are not straightforward, however. Conceptual frameworks offer "a structure, overview, outline, system or plan consisting of various descriptive categories, e.g., concepts, constructs, or variables and the relations between them that are presumed to account for a phenomenon" (Tabak et al., 2018: 74). Having a conceptual frame and accompanying plan in place for how and when these decisions will be made allows for researchers to be systematic in their inclusion and exclusion of survey data during analysis.

To address the issue, an informed process is needed for identifying suspicious cases and removing them. Like the way researchers make arguments for the validity and reliability of their research, fraud is not determined based on a set of rigid criteria that would lend itself well to a checklist format. Rather, researchers can identify evidence to suggest that some cases should be included or excluded from data analysis based on the unique circumstances of their survey.

The reflect, expect, analyze, and label (REAL) framework

We developed our approach to thinking about survey fraud based on lessons learned from conducting online survey research that incentivized participation with monetary honorariums where we encountered high levels of suspected fraud during the eligibility screening survey. We recommend thinking through the issue of survey fraud prior to survey administration and developing a plan for addressing fraud once the survey data are being collected. To do this, we propose a set of guiding questions that help to plan for identifying suspicious survey responses. Furthermore, these guiding questions can help to plan for both types of fraud discussed in the introduction: unique participant fraud (i.e. fraudulent submissions from the same, easily recognizable respondent) and alias fraud (i.e. fraudulent submissions from those seeking to hide their identities). These guiding questions cover the lifespan of a survey. Prior to survey administration, the REAL Framework guides researchers to consider survey vulnerabilities, and identify expected patterns in the data. During data collection, the framework guides researchers to explore how expected patterns match actual data patterns. Finally, during data cleaning and analysis, the REAL Framework guides researchers to systematically apply previously identified criteria to make final determinations about suspicious submissions in order to exclude or include participants in the study (see Table 2 for a summary of our overall framework). The primary intention of this framework is to address suspicious and fraudulent participation in surveys with incentives. However, these tools may also be useful for identifying suspicious survey responses when researchers are not using incentives.

We include a full example of the REAL Framework as it was applied to a screening survey in which we encountered high levels of suspicious responses in Supplemental Appendix A. The survey was directed toward community providers who deliver services to youth with Autism Spectrum Disorder and focused on understanding the practices they are familiar with and utilize to treat their clients (Wainer et al., 2017).

Table 2. Designing a plan for identifying and addressing suspicious survey responses.

Guiding question	Research phase	Issues to consider	Case study examples
Based on your planned recruitment and distribution practices, in what ways might your survey be vulnerable?	Pre-data collection	What resources are available to assess and deal with suspicious responses? What initial strategies can be built into the survey implementation process to address suspicious responses?	Staff time to review responses throughout the process and identify fraudulent participants; screening questions to determine participant eligibility and filter out multiple submissions
What are the patterns you would expect to see in survey data?	Pre-data collection	What would non-suspicious responses look like? Consider: demographic information, responses to substantive survey questions, survey meta data	Email address format, time to complete the survey, time between survey submissions
How do expected patterns relate to patterns in reality?	Data collection, post-data collection	Where did the patterns you expected diverge from those you expected? Are there any unusual patterns that you were not anticipating? Are those divergences enough to warrant suspicion? What evidence suggests that they are suspicious?	Random email address formats, short completion times, short time between surveys or significant overlap between survey submissions at a given time
What level of suspicion is sufficient to exclude data from your survey?	Pre-data collection, data collection, post-data collection	How can you ensure that the same criteria are applied across all survey responses?	Fisher's exact test to assess significant differences in suspected fraudulent responses and full population of responses

REFLECT: based on your planned recruitment and distribution practices, in what ways might your survey be vulnerable? What design elements are built into your study to avoid fraud?

These questions are focused on identifying preventive methods for addressing survey fraud through evaluating vulnerabilities in survey plans. A good starting point is to consider planned recruitment practices. To address *unique participant fraud*, researchers should consider establishing a system to prevent the same individual from participating more than once using the same identifying information. To address *alias fraud*, researchers should consider how widely they plan to engage in recruitment efforts, and how to avoid distributing study eligibility criteria and any associated participation incentives to individuals who would not likely meet criteria for study inclusion. Similarly, when planning recruitment efforts, researchers should consider whether it would be possible for participants to use distributed links more than once.

Researchers at this stage can additionally consider a variety of tools to utilize for issues that may arise during recruitment and data collection phases. These may include utilizing single use links, establishing highly focused recruitment methods, and selectively communicating participation incentives (e.g. only to individuals who are a part of the highly focused recruitment efforts; individuals already indicating interest in participation). At this stage, researchers may also consider implementing practices that will prevent a fraudulent respondent from participating in the study more than once, such as using cookies, CAPTCHA, and/or trick questions.

Each tool a researcher considers employing will have benefits and drawbacks that will influence effectiveness within the context of their particular project. For example, single use links may be challenging if a participant starts a survey and wants to come back to it. Using cookies to identify individuals trying to participate more than once may lead to exclusion of participants who share a computer. Tools like CAPTCHA can be very useful for preventing automated survey responses, but the tasks involved may prevent eligible participants from accessing the survey (e.g. participants whose computers lack audio capabilities may not be able to complete an audio-based CAPTCHA task; Teitcher et al., 2015). Thus, researchers should consider the potential effectiveness of any particular fraud prevention or identification tool within the context of their survey and the population they intend to engage.

Furthermore, researchers may also reflect on the resources they will have available to address survey fraud throughout the study phases. This can help identify approaches that will best match the research team's ability to monitor for fraud. For example, a team with many personnel resources may be able to have multiple individuals engage in follow-ups to check the identity of each respondent through direct contact with the participant or searching for them online. However, this may not be possible in a project with limited resources.

Instead, limited-resource studies may focus efforts on identifying natural opportunities to build in fraud prevention that do not require substantial resources.

Researchers can also consider the sensitivity of the survey topic in considering what indicators would be appropriate to identify suspicious or fraudulent responses. In situations where the focus of a survey is sensitive, researchers may choose to collect very limited identifying information about respondents, avoiding indicators like IP addresses (e.g. Barratt et al., 2015, 2017). In these situations, researchers can consider the demographic variables they do choose to collect and use these in the "expect" stage of the framework to consider patterns in them that would raise suspicion. They can also use question-level indicators (e.g. length of time spent on a survey page or question) as tools for identifying when a participant has not seriously completed the survey. They may additionally choose to employ preventive strategies, for example, using cookies to make it difficult for an individual to participate more than once from the same computer.

EXPECT: what are the patterns that you would expect to see in the survey data? What would be unusual to observe in the collected data?

Although it is impossible to anticipate the full scope of responses that may come from conducting a survey, it is recommended that researchers review literature, speak with recruitment or content experts, and otherwise obtain knowledge of the population that they plan to survey as well as parameters for study inclusion that may help identify suspicious responses. Specifically, considering what patterns or themes are expected in the data before distributing the survey can provide insights during data analysis when patterns and themes are emerging. For example, if the study includes a focus on participants from a certain geographic region, a researcher should expect that survey meta data to reflect this; while some respondents may be traveling elsewhere when completing the survey, it would be unusual to find many participants from other geographic regions completing the survey. Similarly, it would also be suspicious if certain demographic patterns were expected, as is the case when using a targeted sampling approach and responses deviated significantly from the expected pattern (Bietz et al., 2016). For example, if researchers expect high levels of variance in demographics, it would be suspicious to see a single demographic characteristic arising many times. In this case, the researchers may consider how patterns in single variables interact with each other. For example, it may be more suspicious to see multiple survey submissions with the same name that also come from the same IP address and report being the same gender or age than only considering the respondents with the same participant name as being suspicious.

It may also be useful to consider the level of information available regarding the potential sample population. In high information situations, a researcher may have a clear perspective on where participants would be located and what types of demographic information would fit within their understanding of the sample. In lower information situations, a researcher may consider internal survey characteristics, including the length of time spent on a page of the survey or on a particular question relative to the expected time it would take to respond. This can help identify non-serious submissions or automated responses. Although researchers may not have specific information about expected demographics, they may be able to identify expectations that would support future analysis. For example, researchers may consider whether they would expect participants to be co-located (e.g. would it be suspicious if many responses came from the same IP address?) and prepare to check for repeated IP addresses. This can guide analysis for unexpected patterns in the data.

ANALYZE: how do the actual patterns seen in data analysis procedures align with the expected data patterns?

During the data cleaning and analysis phase, researchers can examine whether the study yielded the patterns that were expected or if unexpected patterns arise. This requires an assessment of the data as a whole and provides a basis for raising suspicion about individual cases or groups of cases. What constitutes a suspicious response pattern depends on the context of the survey. For example, when surveying participants who work in the same office, similar or even the same IP addresses would not be suspicious as they may use the same or networked computers to complete the survey. Researchers can conduct several analyses to identify patterns and discern the significance of patterns in things like participant names, IP address frequency, email address domain and name, geolocation mapping, and proximal time clustering of responses.

LABEL: what is the threshold required to label a response as fraudulent and exclude it from your dataset?

Determining the level of suspicion required to label a response as fraudulent and exclude it from analysis is critical. We hesitate to offer a strict set of criteria to label responses for two reasons. First, the Internet is a rapidly changing medium, and as it changes so do aspects of survey research. Second, the circumstantial nature of research would limit usability. Instead, researchers at this stage should be guided by the prior steps in the framework to determine how they will label and exclude fraudulent submissions.

To begin, researchers should consider the robustness of the tools they have access to. That is, how confident can researchers be that their methods are flagging fraudulent submissions rather than legitimate submissions? How confident can researchers be that their methods are not under-identifying fraudulent submissions? In addition, consider whether a participant who provides several survey submissions has added any legitimate data. This will determine whether it is important to remove all submissions from a suspicious individual or to include one of them (e.g. the first submission).

Researchers can use an algorithmic approach, wherein they determine how stringent the criteria will be. Once the criteria are set, multiple people can apply them systematically, allowing for reliability checks. The criteria should also be well documented in case the researchers need to perform an audit of the data at a later date.

Discussion

The purpose of this article was to introduce and demonstrate a framework to guide planning and decision-making for identifying suspicious survey responses in online research, especially online survey research that incentivizes respondents with monetary honorariums. We outlined the approach we applied to a survey involving suspicious submissions and how that approach can be applied to other studies using online surveys. We conclude here with some final lessons learned for applying this approach and some interpretation of the data that we explored for this study.

Using this approach to addressing survey fraud has a number of implications for survey research. It can make it easier for the research team to set realistic expectations early in the data collection process for what resources are available and how they can be applied to address this issue. In addition, it can make it easier for research teams to audit their process and justify their decisions in a clear way. Finally, the process facilitates replication in future iterations of the research.

Considerations for application

Those wanting to apply the REAL framework should keep in mind several considerations as they apply it, including determining logistical needs ahead of survey implementation, considering the ethical issues related to including or excluding data in a study, and considering the issues related to providing incentives for participating in research. Conducting successful online survey research requires many practical considerations, including pre-planning for the need to address fraudulent responses. This means the dedication of resources for addressing the problem before it begins. As it may unfold in unexpected ways, these resources should be flexible enough to adapt to the specific issues that arise.

In addition, decisions about inclusion and exclusion should be considered through an ethical lens, recognizing that any time a legitimate participant is excluded, the researcher has silenced their voice in the study. Thus, consideration of the potential impacts of losing some participant knowledge is critical. Conversely, the inclusion of fraudulent responses diminishes the value of legitimate responses and adds error to the data that can lead to inaccurate results.

Finally, as online research grows in use, there will be more opportunities for fraudulent respondents to participate. Incentives provide one compelling reason to engage with a survey one is not eligible for, so researchers can consider the broad appeal of the incentive they offer and work toward establishing incentives that would not be compelling to those outside of their population of interest. This is unique to each research situation, but within a community context, researchers may offer thanks to participants for their time by providing specific resources, like classroom supplies for teachers. This can replace monetary incentives that may have broad appeal with those that only serve the interests of legitimate participants.

Limitations

Our framework facilitates the systematic process of identifying online survey fraud, but it does not protect against the unknowable approaches that fraudulent respondents will take to access and complete online surveys. Looking back after online surveys are completed, there will always be some information that researchers were not initially looking for that may point to fraudulent responses. In addition, our research focuses specifically on applied settings (e.g. engaging practitioners and community members as participants). Thus, our approach to addressing fraudulent survey responses has primarily been explored within this context.

Future directions

We suggest several future directions for applying and refining the REAL framework. First, to better understand this issue, we encourage more open discussions about the nature and types of survey fraud that researchers encounter in their work. Reporting this information within empirical papers will advance collective knowledge about the types of fraud that may arise around different survey approaches or content areas. While this has been discussed openly in some contexts—for example, with research using Mechanical Turk—further discussions about online surveys across multiple platforms will help others plan for issues they might encounter. These platforms are becoming increasingly popular among researchers and their continued benefits to the field require open conversations about how researchers address survey fraud (Anderson et al., 2019). Much of the work in this area so far has focused on specific methods (without a set of best practices) for addressing fraud when using Mechanical Turk (e.g. Hauser et al., 2019; Hulland and Miller, 2018). Here, we provided a systematic framework

for thinking about this problem over the lifespan of a survey. Future research can explore the impact of the framework on the process of collecting data through Mechanical Turk and related platforms and illuminating the types of issues that arise while doing survey research using these platforms. As evidence advances in this area, researchers may consider developing a refined checklist to support decision-making regarding fraudulent and suspicious submissions. Such a checklist could be developed and refined through a similar process as that used for developing the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines (Liberati et al., 2009). Such a checklist could support consistency in the process for identifying fraudulent and suspicious submissions as well as consistency in reporting. Second, while exploring the issue of survey fraud in our own research, we began to note patterns suggesting that fraudulent responses may sometimes come from networks of individuals sharing information about online surveys. Future research should explore how information about online surveys gets circulated beyond initial recruitment and how social connections may play a role in who is able to access information about online surveys. Third, researchers should explore the reasons why fraudulent respondents target online surveys and consider how to build in additional affordances to their studies to disincentivize fraudulent participation. Beyond things like making it difficult for participants to receive incentives they are not qualified for, researchers may explore the role of social influence theory to understand how groups of connected individuals choose to participate in online surveys when they are aware they are ineligible (Bagozzi and Lee, 2002). For example, participants on large-scale platforms sometimes use forums to communicate with each other and these spaces may promote social influence, setting norms in favor of or in opposition to engaging in fraudulent activities. Exploring reasons why ineligible individuals try to participate can facilitate identification of additional strategies for preventing survey fraud.

Finally, researchers can explore other quantitative approaches to assessing the extent and impact of fraudulent survey responses on the outcomes of studies. For example, research on p-curves allows for comparisons of research that is both published and unpublished in order to identify and correct for inflated effect sizes (Simonsohn et al., 2014, 2015, 2016). A similar approach can help identify research that includes a high rate of survey fraud. This could be particularly useful for identifying fraud in published and could be useful for informing how research is included in systematic reviews or meta analyses.

Conclusion

In this article, we established the importance of considering survey fraud as an issue for online survey research and have presented our framework for addressing fraud. We suggest that researchers consider fraud as an issue over the lifespan of their survey and apply the questions we present to address the issue throughout. Future studies can provide insights into the extent to which this issue occurs throughout social research, further applications of this framework, and the impacts of fraudulent participants on study outcomes.

Acknowledgements

The Usual Care for Autism Study Consortium comprised (in alphabetical order) Elizabeth Cohn (CUNY-Hunter), Amy Drahota (Michigan State University), Connor M Kerns (University of British Columbia), Matthew D Lerner (Stony Brook University), Lauren Moskowitz (St. John's University), Latha Soorya (Rush University Medical Center), and Allison Wainer (Rush University Medical Center).

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 funding from the Adelphi Center for Health Innovation, Pershing Charitable Trust, and the Brian Wright Memorial Autism Research Fund.

ORCID iDs

Jennifer Lawlor https://orcid.org/0000-0003-2857-3030
Amy Drahota https://orcid.org/0000-0003-1169-3546

Supplemental material

Supplemental material for this article is available online.

References

Anderson CA, Allen JJ, Plante C, et al. (2019) The MTurkification of social and personality psychology. *Personality and Social Psychology Bulletin* 45(6): 842–850.

Aust F, Diedenhofen B, Ullrich S, et al. (2013) Seriousness checks are useful to improve data validity in online research. *Behavior Research Methods* 45: 527–535.

Bagozzi RP and Lee KH (2002) Multiple routes for social influence: The role of compliance, internalization, and social identity. *Social Psychology Quarterly* 65(3): 226–247.

Barratt MJ, Ferris JA, Zahnow R, et al. (2017) Moving on from representativeness: Testing the utility of the global drug survey. *Substance Abuse: Research and Treatment* 11: 1–17.

Barratt MJ, Potter G, Wouters M, et al. (2015) Lessons from conducting trans-national internet mediated participatory research with hidden populations of cannabis cultivators. *International Journal of Drug Policy* 26(3): 238–249.

Bauermeister JA, Pingel E, Zimmerman M, et al. (2012) Data quality in HIV/AIDS web-based surveys: Handling invalid and suspicious data. *Field Methods* 24(3): 272–291.

Bethlehem J (2010) Selection bias in web surveys. *International Statistical Review* 78(2): 161–188.

Bietz MJ, Bloss CS, Calvert S, et al. (2016) Opportunities and challenges in the use of personal health data for health research. *Journal of the American Medical Informatics Association* 23(e1): e42–e48.

Bowen AM, Daniel CM, Williams ML, et al. (2008) Identifying multiple submissions in internet research: Preserving data integrity. *AIDS and Behavior* 12(6): 964–973.

Chandler JJ and 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.

Evans JR and Mathur A (2018) The value of online surveys: A look back and a look ahead. *Internet Research* 28(4): 854–887.

Gosling SD, Srivastava S and John OP (2004) Should we trust web-based studies? A comparative analysis of six preconceptions about internet questionnaires. *American Psychologist* 59(2): 93–104.

Hammond N (2018) Researching men who pay for sex: Using online methods for recruiting and interviewing. *Methodological Innovations* pp. 1–11.

Hauser D, Paolacci G and Chandler J (2019) Common concerns with MTurk as a participant pool. In: Kardes FR, Herr PM and Schwarz N (eds) *Handbook of Research Methods in Consumer Psychology*. New York: Routledge, pp. 319–337.

Hulland J and Miller J (2018) "Keep on Turkin'"? *Journal of the Academy of Marketing Science* 46(5): 789–794.

Jones MS, House L and Gao Z (2015) Respondent screening and revealed preference axioms: Testing quarantining methods for enhanced data quality in web panel surveys. *Public Opinion Quarterly* 79(3): 687–709.

Konstan JA, Rosser BRS, Ross MW, et al. (2005) The story of subject naught: A cautionary but optimistic tale of internet survey research. *Journal of Computer-Mediated Communication* 10(2): 11.

Liberati A, Altman DG, Tetzlaff J, et al. (2009) The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: Explanation and elaboration. *Journal of Clinical Epidemiology* 62(10): e1–e34.

Muir JA and Van Oorschot PC (2009) Internet geolocation and evasion. *ACM Computing Surveys* 42(1): 1–23.

Mustanski BS (2001) Getting wired: Exploiting the internet for the collection of valid sexuality data. *The Journal of Sex Research*: 38(4): 292–301.

Nosek BA, Banaji MR and Greenwald AG (2002) E-research: Ethics, security, design, and control in psychological research on the internet. *Journal of Social Issues* 58(1): 161–176.

Oppenheimer DM, Meyvis T and Davidenko N (2009) Instructional manipulation checks: Detecting satisficing to increase statistical power. *Journal of Experimental Social Psychology* 45(4): 867–872.

Palamar JJ and Acosta P (2020) On the efficacy of online drug surveys during the time of COVID-19. *Substance Abuse* 41(3): 283–285.

Pequegnat W, Rosser BRS, Bowen AM, et al. (2007) Conducting internet-based HIV/STD prevention survey research: Considerations in design and evaluation. *AIDS and Behavior* 11: 505–521.

Reips U (2000) The web experiment method: Advantages, disadvantages, and solutions. In: Birnbaum MH (ed.) *Psychological Experiments on the Internet*. San Diego, CA: Academic Press, pp. 89–117.

Reips U (2002a) Internet-based psychological experimenting: Five dos and five don'ts. *Social Science Computer Review* 20(3): 241–249.

Reips U (2002b) Standards for internet-based experimenting. *Experimental Psychology* 49(4): 243–256.

Reips U, Buchanan T, Krantz J, et al. (2015) Methodological challenges in the use of the internet for scientific research: Ten solutions and recommendations. *Studia Psychologica* 15(2): 139–148.

Ryan TJ (2018) Data contamination on MTurk. Available at: http://timryan.web.unc.edu/2018/08/12/data-contamination-on-mturk/

Schmidt WC (1997) World-wide web survey research: Benefits, potential problems, and solution. *Behavior Research Methods* 29(2): 274–279.

Simonsohn U, Nelson LD and Simmons JP (2014) P-curve and effect size: Correcting for publication bias using only significant results. *Perspectives on Psychological Science* 9(6): 666–681.

Simonsohn U, Nelson LD and Simmons JP (2016) P-curve won't do your laundry, but it will distinguish replicable from non-replicable findings in observational research: Comment on Bruns & Ioannidis (2016). *PLoS One* 14(3): e0213454.

Simonsohn U, Simmons JP and Nelson LD (2015) Better p-curves: Making p-curve analysis more robust to errors, fraud, and ambitious p-hacking, a reply to Ulrich and Miller (2015). *Journal of Experimental Psychology: General* 144(6): 1146–1152.

Tabak RG, Chambers DA, Hook M, et al. (2018) The conceptual basis for dissemination and implementation research: Lessons from existing models and frameworks. In: Brownson RC, Colditz GA and Proctor EK (eds) *Dissemination and Implementation Research in Health: Translating Science to Practice* (2nd edn). New York: Oxford University Press, pp. 73–88.

Teitcher JE, Bockting WO, Bauermeister JA, et al. (2015) Detecting, preventing, and responding to "fraudsters" in internet research: Ethics and tradeoffs. *The Journal of Law, Medicine & Ethics* 43(1): 116–133.

Wainer A, Drahota A, Cohn E, et al. (2017) Understanding the landscape of psychosocial intervention practices for social, emotional, and behavioral challenges in youth with ASD: A study protocol. *Journal of Mental Health Research in Intellectual Disabilities* 10(3): 178–197.

Wright KB (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): 1034.

Wyatt JC (2000) When to use web-based surveys. *Journal of the American Medical Informatics Association* 7(4): 426–430.

Author biographies

Jennifer Lawlor, Ph.D. is an Associate Researcher at the University of Kansas in the Center for Community Health and Development. Dr. Lawlor uses a combination of community-engaged and computational approaches to study how communities collaborate and

share information to address complex problems, particularly in the context of community coalitions and collaboratives.

Carl Thomas holds a Bachelor of Science degree in Psychology from Grand Valley State University and has served as research assistant for Dr. Amy Drahota at Michigan State University.

Andrew T Guhin is a former graduate research assistant for Dr. Amy Drahota and holds a masters degree in Ecological/ Community Psychology from Michigan State University.

Kendra Kenyon is a former undergraduate research assistant for Dr. Amy Drahota's ACT Lab. She earned her Psychology bachelors degree in Psychology from Michigan State University in 2019.

Matthew D. Lerner, Ph.D. is an Associate Professor of Psychology Psychiatry, & Pediatrics in the Department of Psychology at Stony Brook University, where he directs the Social Competence and Treatment Lab. He is a Founder and Research Director of the Stony Brook Autism Initiative, and Co-Director of the Stony Brook LEND Center. Dr. Lerner's research focuses on understanding emergence and "real world" implications of social problems in children and adolescents (especially those with Autism Spectrum Disorders [ASD]), as well as development, evaluation, and dissemination of novel, evidence-based approaches for ameliorating those problems.

The Usual Care for Autism Study (UCAS) Consortium involves researchers from multiple sites in the United States and Canada, representing diverse geographical regions, socioeconomic status (SES), and urban/suburban/rural designations. The ultimate goal of the UCAS Consortium is to develop a comprehensive understanding of the landscape of intervention practices being utilized by the array of community-based providers and provider attitudes toward the treatment of social difficulties, anxiety, and externalized behaviors for school-aged autistic youth in usual care, community-based settings.

Amy Drahota, Ph.D., is an Assistant Professor at Michigan State University. Dr. Drahota conducts mental and behavioral health services and dissemination and implementation science research focusing on the development and testing of organizational interventions promoting adoption, implementation, and sustained utilization of evidence-based practices for individuals on the autism spectrum