Predatory publication of AI-generated research papers

Lizzie Burgiss, Ben Tatum, Christopher Henshaw, Madison Boswell and **Alan J. Michaels**
{lizzieburgiss,btatum26,chenshaw,maboswell,ajm}@vt.edu
Virginia Tech National Security Institute

Abstract

In an academic ecosystem where faculty face a "publish or perish" mantra, there are distinct openings for predatory publishers. Defined loosely, these are journals who value profits over scholarly cultivation and prey upon unsuspecting authors. Prior research has built lists of suspected predatory publishers to inform colleagues of risks, yet few quantify common characteristics exhibited by these publishers. To test hypotheses around these journals, we probed the behavior of 256 suspected predatory journals drawn from Beall's and Kscien's lists. Using active open source intelligence techniques, we tested the existence and extent of review processes, publication fees, operating location, and communication patterns. We submitted five different ChatGPT4-authored papers to our targeted publishers – these papers were accepted and/or published by 55 journals. By characterizing the responses, we developed a journal assessment rubric to aid authors seeking to publish their work. In the process, we also identified a presumptive shadow network of publishing companies using these practices based on analysis of websites, addresses, and shared employees. All underlying data for our study is open sourced for other researchers to draw their own conclusions.

1 Background

Jeffrey Beall is widely known as the originator of a database of questionable academic publishers seeking to educate and caution colleagues about questionable business practices. In 2010, he coined the term "predatory journals," referring to journals and publishers with fraudulent peer review processes (Muhialdeen, et. al., 2023). Under legal pressure, Beall stopped working on the list in 2016, and an anonymous author has since taken over. Although the list is periodically updated, the number of candidate publishers grows and changes too fast for a single caretaker to maintain. Beall's list highlights elements of a publisher's website that suggest predatory intent such as a homepage that targets authors rather than individuals seeking academic outputs and solicitation for manuscripts via email. In addition, websites may omit details of their review process (Beall, 2012). Suspect websites often promise a rapid publication process, yet without a defined retraction policy.

Other predatory publishers databases include *Kscien's list*, a recently updated database with the broadened goal of identifying questionable publishers. Kscien deems predatory journals "amateurish, greedy, negligent, entrepreneurial entities with the unique ambition of compiling fees from the pockets of naive researchers" (Muhialdeen, et. al., 2023). *Predatory Reports* provides a list of publishers compiled by volunteers, all of whom were harmed by practices of such publishers and wish to educate fellow researchers, promote integrity in academic publishing, and build trust between publications and authors (Das and Chatterjee, 2018). Taking a different approach, *Retraction Watch* built a database of retracted academic papers and their authors, ranking them in order to provide public data on paper retraction for prospective authors (Marcus, et. al., 2024). Their leaderboards include the *Mass Resignations List*, the *Top 10 Most Highly Cited Retracted Papers*, and a *Retraction Leaderboard*. Taken in aggregate, these websites laid the groundwork for our early identification of candidate predatory publisher websites for evaluation.

Predatory publishers use verifiable tactics to pull in authors. They may use superfluous wording to appear more reputable, or extremely succinct to the point of appearing unprofessional (Talari and Ravindran, 2023). They may advertise themselves extensively, or choose a name purposely similar to that of a well known journal. Other problematic symptoms are acceptance of a paper in less than a week or asking for no revisions, as both are indicators of poor peer review processes. Sometimes, publishers obfuscate the review process with no

Proceedings of the 1st International Conference on NLP & AI for Cyber Security, pages 1–9
July 29–30, 2024.

receipt of a confirmation or communication with an actual assigned reviewer (Happe, 2020). Transparency of publication fees is also essential, as it builds trust between an author and publisher in addition to being an ethical way of proceeding with transactions. This transparency can also help to alleviate an author's suspicion that their acceptance decision was influenced by the monetary transaction involved (Laine and Winker, 2017).

For the purposes of this paper, we will use the working definition that predatory publishers are those that appear to value publication fees over academic merit and whose peer review process lacks sufficient academic rigor. While there are numerous aspects that any such publisher may possess, at the core of all mentioned traits is the motivation for publication fees. The key distinction thus lies in the publishers' motivation.

Just as the definition of predatory publishers is contended, so is the usefulness and validity of lists such as Beall's and Kscien's. Some authors and librarians argue against this genre of index in defense of low-tier journals. Some researchers accuse Beall of methodological flaws, personal bias, and discrimination against developing economies (Yeates, 2017). Others highlight the occurrence of false positives, the tricky case of expedited reviews, the appeared bias against international dialects, and the nuance of publisher locality (Kimotho, 2019). Finally, differing concepts of quality, privilege in scholarship, and "academic centre and periphery" are noted in arguments against such indexes of predatory publishers that may often capture low-tier journals in the crossfire (Bell, 2017).

The actual identification of predatory publishers is one subject of debate, and in some cases, court proceedings. The identification of predatory journals is an ongoing effort as vetting journals is a long and subjective process. Current tools for identifying predatory journals act as resources for academic authors to protect themselves from journals that are simply for-profit companies. These tools include *Cabell's Predatory Reports* an online service that offers reviews of journals authors wish to consider. The process for a prospective author includes a personalized quote resulting in access to an account dashboard with predatory weighted scores (Das and Chatterjee, 2018). Free resources include Loyola Marymount University's *Journal Evaluation Tool*, Think Check Submit's checklist, and related rubrics. (Cortegiani and Shafer, 2018; Rele et al., 2017; Insight, 2023; Eaton, 2018). These rubrics work well for publishers that are verifiably legitimate or predatory, but not as well for classifying those that may fall into the gray area in between. Furthermore, the constant reorganizing of predatory publishing houses quickly renders efforts outdated. To-date, scrutiny of publishers requires extensive manual review, preventing the formation of a reliable, real-time, or comprehensive list of predatory publishers (Schlesselman-Tarango, 2024). Our study aims to provide open-sourced quantitative data and an evaluation rubric that produces identification tools that support rapid case-by-case evaluation of potentially predatory academic journals.

The following sections include our experimental setup creating the publisher's submission pool, analysis of results, a journal evaluation rubric summarizing observations, and conclusions with recommendations for future research. All data generated and collected for this study are made available to other researchers (Burgiss et al., 2024). The key contribution of this paper is an evaluation rubric using quantitative evidence on journal behaviors. In collecting the evidence for this endeavor, we have also performed a bit of investigative journalism, identifying connections between publishing companies previously involved in making millions from questionable sites (Deprez and Chen, 2017; Federal Trade Commission, 2020).

2 Experimental design

To quantify publisher behaviors, our study submitted fake papers to suspected predatory journals. Recognizing Kscien's list as a super-set of Beall's, we drew our list of publishers and subsequently journals from Kscien's list (Muhialdeen, et. al., 2023). Kscien's list totaled 1,298 publishers and journals as of 05/18/2023. Although this list is extensive, we reduced the list to include only journals with cyber-aligned topics such as computer science, business IT, science, or engineering. This reduction led to the targeted 256 publishers. No other criteria or limitations were placed on the selection.

A maximum of three journals per publisher were allowed for our submission pool to ensure adequate diversity and minimize impact on legitimate review processes. Paper topics were also randomized before submission. A sample of the themes is shown in Figure 1, and a full list of submissions can be found in the appendix content (Burgiss et al., 2024). To help ensure the integrity of our own results and to offer the research community access to the underlying methodology, we have open sourced all the resulting artifacts (anonymizing some identifying information) (Burgiss et al., 2024). We would like to note our commitment and intent for ethical experimental design, stressing that fake papers were only sent to publishers appearing on community lists of predatory publishers. Our experiences with ChatGPT suggest that it would be capable of co-authoring semi-believable papers with more human input and iteration, which would be better suited to penetration testing of non-predatory, albeit low quality, journals that are expected to incorporate expert review.

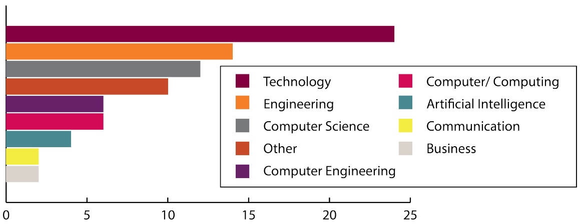

Figure 1: Breakdown by topic of all journals submitted, highlighting the engineering topic category.

We constructed five AI-generated conference-length papers that pass superficial scrutiny. The titles include *Optimizing Bubble Sort*, *Prompt Engineering Framework*, *Randomized Fake Identities*, *Fraud Detection with Fake Identities*, and *Automated Clock-in Reminder System*. The diversity in the papers topics was to avoid a publisher lacking a rigorous peer review process to identify the correlation. Our papers were developed using ChatGPT and the prompts and response logs are available as part of our open source data (Burgiss et al., 2024). The results of the abstract and experimental design generation phase varied from extremely convincing to weak and wordy arguments. We initially tested each prompt with ChatGPT 3.5, incrementally refining the papers with human-in-the-loop prompts to ChatGPT 4. Our intent was to create documents with sufficient content that a novice might accept as legitimate, while anyone with a bachelor's level education in the appropriate field would recognize the inherent lack in scholarly value.

A key takeaway from our AI prompting is that it is essential to outline the product you wish to create, then further prompt extrapolation until the desired results are achieved. The more technical information provided in the prompt, the more technical the answer became. Each AI prompt topic included key words and ideas pertaining to the subject and began by asking for a hypothetical abstract on the topic. In addition, ChatGPT responds best when the questions being asked are an incremental rewording of its previous answer. Working in this manner, an initially convincing paper can be built entirely with AI generated elements such as code, data, and citations. When read with any attention to detail, however, our fake papers contain verbose rambling with little substance and impossibly positive results. In addition, they contained blatant grammatical errors, formatting issues, and citation problems. Most notably, all citations in the paper are entirely falsified, which can be easily verified.

A critical element in all papers are the few and fake citations. The prompt for these was provided as follows: "could I have 5 fictitious citations relating to the paper in BiBTeX format." Notably, ChatGPT always provides a warning when providing these false citations: "please note that these citations are fictional and generated for illustrative purposes only. Make sure to replace them with appropriate and accurate citations based on actual sources when writing your research paper." ChatGPT is aware of its use in falsifying information, as it suggests an effort to avoid such behaviors.

As an extension of our overarching research project, *Use & Abuse of Personal Information*, the team built a signup engine for a mock user database (Harrison et al., 2021). The database fields were generated to mimic demographics similar to the United States through the use of official government records such as US census data. All traceable information such as addresses are designed to mimic reality, but do not contain any real personal information in order to protect individuals and organizations from accidental identity impersonation as shown in Figure 2. The development and further experimental use of this software are documented in the associated papers (Michaels and George, 2021; Harrison et al., 2021). Armed with identities, papers, a signup engine, and data collection tools, we proceeded with controlled distribution of the papers for evaluation by potentially predatory journals.

3 Results and data analysis

Our process entailed collecting information on our publishers and journals such as URLs, operating locations, and website appearance. We then collected emails received in response. The emails were manually read and assigned to categories based on their

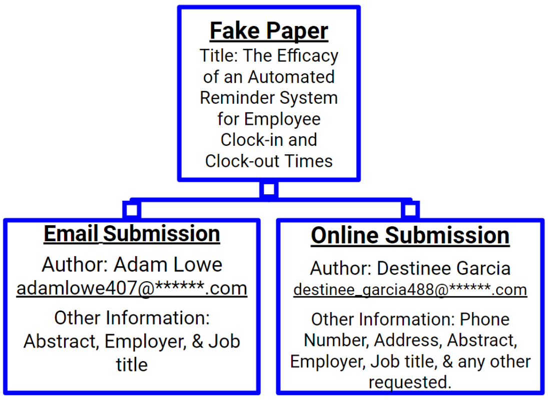

Figure 2: Visual representation of sign-up event.

primary topic of discussion: acknowledged submission, rejected submission, request to complete more steps accepted submission, and request for payment. The following analysis is the result of statistical significance and qualitative observations made from the collected emails and publisher attributes. Submissions were performed according to the request of the journal. 41% were submitted via email and the other 59% were submitted though online portals. An email address was given for all submissions connecting to our email server. Every identity asked to be sent all possible communications from the publishers to their respective email address. Emails received were evaluated for red flags, domain changes, similar websites, geographic locations, submission outcomes, and other notable occurrences. The relevance of each subsection is intended to be a different identifier for potentially predatory publishers. They have been subsequently compiled into a rubric for use by authors to assess the nature and intent of academic publishers in the following section.

3.1 Predatory journal red flags

Exploring the trustworthiness of journals under consideration, we found multiple traits as potential identifiers of predatory behavior. The first is whether or not the journals accept a meritless paper. The second class of indicators is how quickly publishing costs arise, and moreover whether prices are excessive or given at a discount. The interconnected nature of journals and their editorial staffs, including red flags as to other publicly identifiable links, is a third indicator. Finally, we sought to identify acceptable levels and types of communication a journal has with an author.

3.2 Domain changes

Throughout the research, multiple publisher domains on Kscien's list changed. Sometimes the publisher simply changed their web domain name, while in other instances they became entirely unavailable. During our six-month experiment, 38 domains changed from a publisher to another site type as shown in Figure 3. Note the 28.9% turnover of journal domains to gambling content, as it is the second largest category after the journal site displaying a 404 error message. This suggests that there may be connections between predatory publishers and gambling content involved in a lawsuit.

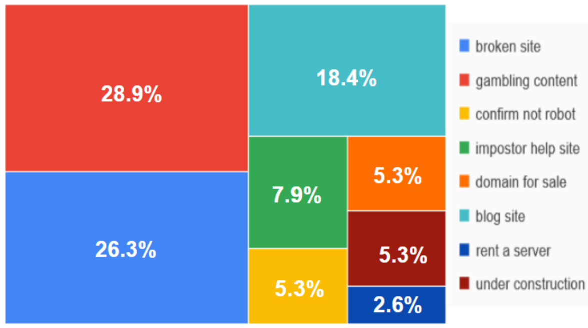

Figure 3: Breakdown of 38 changed web domains for suspect publishers during our six-month experiment.

As an example, *International Association of Multidisciplinary Research (IAMURE)* is listed on Beall's list with URL iamure.com. IAMURE's domain has since transitioned to gambling advertisements provided by SunCity, which has had its own share of legal troubles (O'Connor, 2023). In November of 2021, SunCity was party to a lawsuit resulting in the founder being sentenced to 18 years in jail and being ordered, along with his co-defendants, to pay the Chinese government a fine of $830 million in addition to financially compensating various casino operators.

3.3 Locations: an interconnected web

When assessing our publishers for applicable journals prior to submission, we noticed that English is likely not the native language of the individuals sometimes creating these sites. This was suggested by poor grammar, spelling, and misuse of words as observed on websites and in email communications. For this reason, we explored journals' operating locations by collecting the office addresses listed on their website for analysis. Location data taken from publishers' websites presented several hot-spots (see Figure 4). These included New York

City and London as the most dense with central California, southern India, and the United Arab Emirates as secondary clusters.

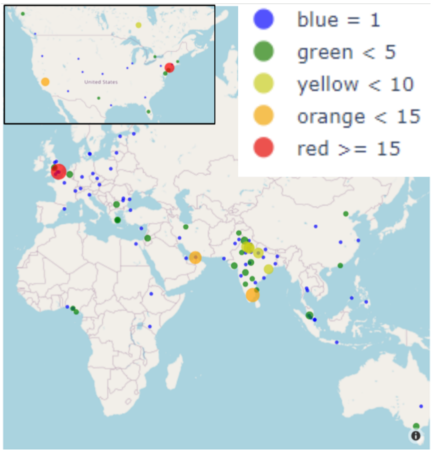

Figure 4: Operating addresses of suspect publishers.

Aggregating these locations, we noticed several patterns, which led to a web of online documentation stemming from business addresses and identified specific individuals as key players ultimately linking multiple publishing companies. These relationships suggest an active worldwide network connecting many of the suspect publishers in this study as well as others on Kscien's list.

After researching a commonly listed address we identified a second common address as presumptively residential. We also found overlaps in employees from different journals, and one case, identified a journal director who rotated frequently between several journals. We also identified further unexpected journal company overlaps (Datalog, 2023; Company, 2023; Robert, 2024; Insight, 2023; Eskildsen, 2024; Search, 2022; Companies London, 2024; USA, 2024). Using these public data sources, we validated the connections and uncovered an interconnected web of suspect publishers as captured in Figure 5. This subset represents only a fraction of publishers, locations, and individual actors. This method of sharing assets to possibly perpetuate less than ideal peer review practices has the capacity to further infect the academic publishing space. These entities value monetary profit over supporting authors and positively furthering the academic research publishing community.

Previous court cases led to multi-million dollar judgements against entities of OMICS Online (Federal Trade Commission, 2020). Considering that these practices appear to remain active even after \$50.1 million penalties, there is serious money at stake for such behaviors to continue. Our fake papers were in fact accepted to four journals connected to OMICS Online.

3.4 Submission outcomes

Of the 256 fake papers submitted, 141 received one or more emails while the remaining 115 received zero communication after submission. The 141 identities who were communicated with received a total of 588 emails resulting in an average of four per account. Sixty-one of the identities were asked to complete a further step other than payment which suggests at least a basic peer review process. The total number of emails received requesting further steps was 176. Forty-two submissions were immediately asked for a payment ranging from \$30 to \$2,599. The mean publication fee of accepted papers who requested payment was \$618.43, while for the no decision and rejected category the mean was \$282.57. Two of the highest prices (\$1674.93 and \$2229.48) came from OMICS Online journals. For these 42 submissions, payment was requested regardless of paper acceptance. Several publishers followed up their initial requests for publication fees with steep discounts (40%-94%) after we did not respond to first requests for payment. Further data is listed in the appendix (Burgiss et al., 2024).

Of the 141 submissions with responses, 76 were never notified of an acceptance decision. Fifty-five were sent an acceptance letter, and ten received a rejection letter as shown in Figure 6. This practice of sending a full rejection letter indicates both a higher level of value placed on the author and professionalism as well as more established decision and review processes. The fact that our fake papers received rejections from some journals therefore shows their review processes do have academic merit. This also confirms, along with other testing, that ChatGPT papers were identifiable as not having enough merit to be published.

One surprising result was the similar acceptance percentage of papers submitted online versus by email. We expected that publishers who requested submissions via email would be more likely to be predatory, yet this hypothesis was inconclusive. Email submissions led to a 36.2% acceptance rate (21 of 58), while online submission portals had a 44.6% acceptance rate (37 of 83). Therefore, the mode of submission does not appear to be a strong indicator of journal credibility, but rather a potential a sign of editor resources or indicative

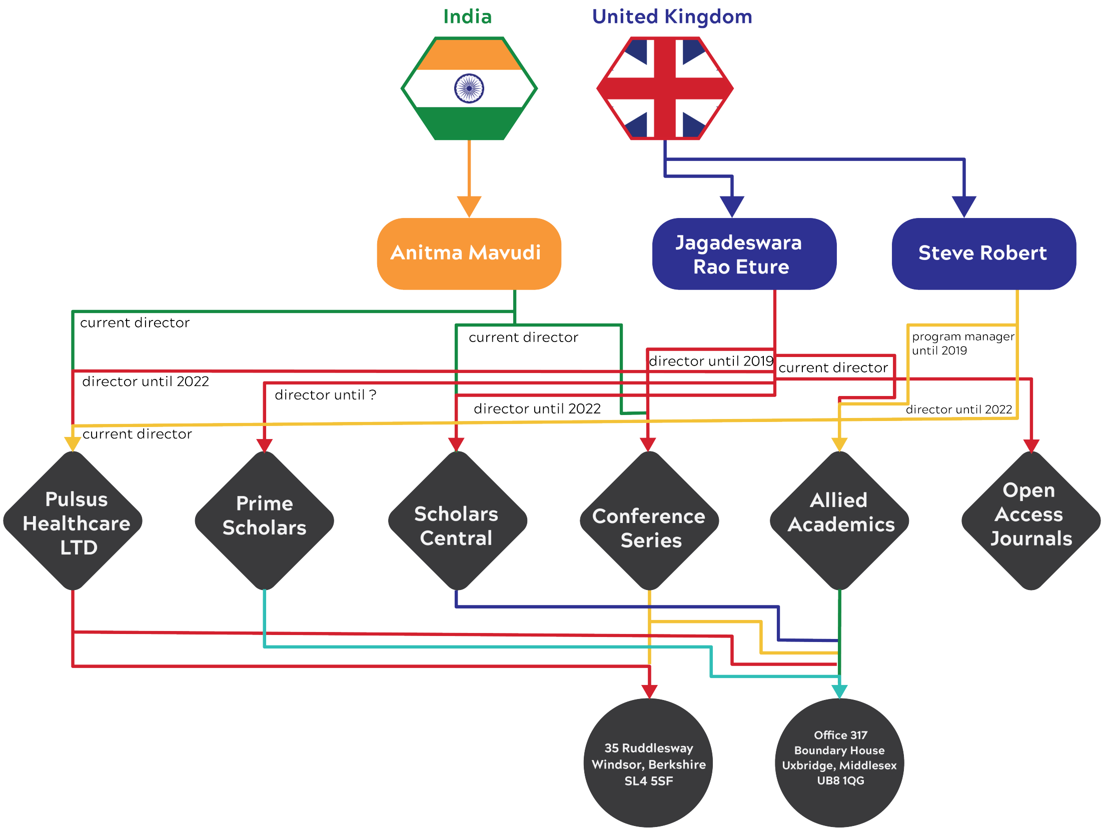

Figure 5: Identified web of journals between various OMICS Group Inc. sub-companies.

	Email Submission	Online Submission	Total Submitted
Accepted	21 (8.20%)	37 (14.45%)	58 (22.66%)
Rejected	2 (0.78%)	5 (1.95%)	7 (2.73%)
Acknowledged	35 (13.67%)	41 (16.02%)	76 (29.69%)
No Response	63 (24.61%)	52 (20.31%)	115 (44.92%)
Total Submitted	121 (47.27%)	135 (52.73%)	256 (100%)

*percentages represent the portion of all submitted papers

Figure 6: Data on the acceptance status of all papers, including a breakdown by submission method.

of more human interactions as opposed to a more automated process.

3.5 Other notable occurrences

One journal, *European Journal of Engineering and Technology Research*, rejected our paper for plagiarism. This is somewhat surprising, but perhaps also shows the limitation of ChatGPT to generate unique content. Three journals *(Institute for Digital Forensics and Cybercrime Studies, European Journal of Electrical Engineering & Computer Science, Studies in Engineering and Technology)* stated that they ran plagiarism reports and came up with 2%-3% reuse (i.e., practically no reuse). Given the use of ChatGPT to generate the papers, we did not expect blatant plagiarism, yet evidently some detection methods are more robust than others. This highlights the need for AI generation detection scoring to become a part of peer-review processes if not already implemented, as our papers scored 87% - 99% chance of being AI generated when we tested with multiple free online tools.

Multiple journals sent PDFs with our formatted papers or private links to the formatted papers (Burgiss et al., 2024)(Thomas, 2022). However, one journal published our paper without payment or any further interaction other than initial online submission (Thomas, 2022). On one hand, this may display a commitment to open access publications by requiring no publication fee and no access fee. However, concerns arise such as an author's consent to publish, the extremely quick turn-around in publication, the lack of request for edits, and the lack of further communication before publication.

3.6 Trends in acceptance

We categorized five clear trends in the responses to our papers: emails asking for further steps, excessive emailing, requesting payment multiple times, publication fee discounts, and payment amount, which are further explained in the rubric and Figure 8. A further representation of the grouping and statistical significance of each trait is shown in Figure 7.

Criteria	Accepted	Rejected & No Decision
More Steps Emails	>1/accepted 17/58 (29.31%)	>1/no decision 8/83 (9.64%)
Excessive Emailing	4+/accepted 27/5 (46.55%)	4+/no decision 1/83 (0.01%)
Requesting Payment	>1/accepted 23/58 (39.66%)	>1/no decision 1/83 (1.20%)
Offering a Discount	3/58 (5.17%)	0/83 (0.0%)
Payment Amount	20/58 (34.48%)	4/83 4.82%

Figure 7: Statistical significance of rubric criteria as indicated by our fake papers' data.

4 Rubric

Using the results of this experiment, we sought to construct a quantitative rubric that potential authors can use as a guide to evaluating publishers. We have also evaluated all of the journals used in this study (*both those who accepted and rejected our fake papers*) as proof of utility as shown in Figure 9. In order to construct the rubric, we consolidated the common traits among predatory publishers as mentioned above and attempted to translate their statistical difference to a point system as seen in Figure 7. After adjustment according to other qualitative observations, this resulted in the overall point distribution as shown in Figure 9.

We acknowledge that this study only passively collected emails, so a more thorough experiment might integrate human or machine responses to received communications in order to better identify publisher actions that go beyond auto-acceptance.Using this preliminary rubric, our suggestion is to expand by incorporating existing qualitative research on predatory publishing behaviors such as those highlighted in the predatory publishing rubric of *Think, Check, Submit*, as well as Loyola Marymount University's *Journal Evaluation Tool* (Cortegiani and Shafer, 2018; Rele et al., 2017). A more expansive study could help dial in better quantified scores as described in the future work section. After using the rubric instructions seen in Figure 8, move on to the following score ranges. For scores of 2-10, you may proceed but note the observation of some qualities possessed by predatory journals. For scores of 11-20, proceed with high caution but do not proceed if you observe signs the publisher only cares about fees or that they lack a throughout peer review process. Finally, for scores of 20 or higher, do not proceed as you have extensive indicators of predatory practices.

Criteria	Description	Point Value
More Steps Emails	The publisher is sending you multiple emails requesting that you complete the same next step of the process.	2 points: ________
Excessive Emailing	The publisher is sending you more that four emails in a row without your response.	6 points: ________
Requesting Payment	The publisher has sent an email asking that you pay the publishing fee more than once.	7 points: ________
Offering a Discount	The publisher has offered you a discount to the publication fee.	9 points: ________
Payment Amount	The publishing fee is more than $300 USD.	5 points: ________
Instructions: To use this rubric, add the point value for each criteria met during the publishing process. Your total points is a warning score which can be used alongside the Warning Levels chart for personal assessment of predatory nature.		score: ________

Figure 8: Translated penalty scores of common behaviors of predatory journals into a rubric for author's use.

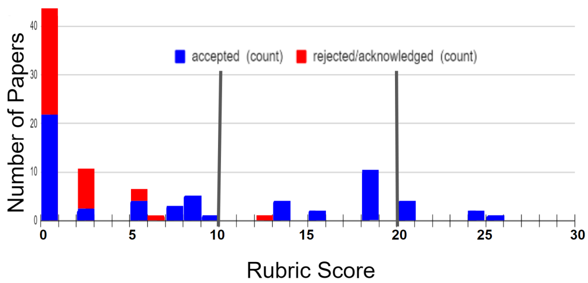

Figure 9: Predation scores of experimental journals.

4.1 Lessons learned

As we learned throughout the process of this study, the research of predatory publishers is all about pre-planning and identifying general targets. The realm of online lists of potentially predatory publishers is extremely vast, and therefore we recommend recognizing personal expertise and sequentially identifying the subset in which you wish to scrutinize. For example, combing though all of Beall's list to identify one regularly-appearing trait is tedious and in some cases pointless work. If those lists were also categorized by expertise area, then the search would be much quicker. Then, before an analysis of the publisher pool, consider a small proportional subset and scrutinize those publishers for commonalities that come in any and all forms quantifiable. These such traits can then be identified by a researcher, and the process is therefore greatly simplified. One specific trait that our team finds especially interesting is how the publishers' domains change over time. We wish to explore research on this in the future. Another interest is in the subset of journals which are subsidiary companies of OMICS group. If working, we would have for each paper submitted a phone number and had a resulting catalog of all the voicemails, calls, and SMS messages received. This additional data might offer further insight into the qualities of predatory publishers.

5 Conclusions

In order to investigate the predatory nature of suspected publishers we submitted AI-generated academic papers to suspected predatory publishers that had journals under the cyber umbrella. We collected journals' operating address, all emails received from them, and their URL, among other general information. We then started to notice overlaps in locations of these companies which led us to further overlaps in employees of the publishers. In observing URLs, we found that almost 30% of URL turnover resulted in gambling content that had ties to a formerly charged company, SunCity. In addition, we learned that some publishing companies in our study are sub-companies of the publisher and academic conference company OMICS Group Inc. which was involved in an $50.1 million Federal Trade Commission lawsuit. After thorough data analysis, and with the knowledge of our experiences in receiving both rejections and acceptances of our fake papers, we put together a rubric for fellow academic writers. Our aim is to provide a resource that can guide authors in their personal assessment of academic journals that they may wish to publish with. We then further proved our rubric by assessing the publishers involved in our own study. This research offers concrete insights into the processes of knowledge management underlying scholarly publications, as well as groundwork for more comprehensive indicators of predatory publishing practices.

6 Future work

To further the capabilities of identifying predatory publishers, researchers must both build on the foundations laid by existing databases such as Kscien's and Beall's, but also remain flexible in order to identify new traits. This paper demonstrates the viability for correlation of quantifiable characteristics for suspect journals with their qualitative categorization as *predatory*. Transforming the present experiment to one that includes fake ID responses up to the point of payment could offer better insight into red flags beyond the point of submission. With such a diversified list of criteria, a more reliable and widely-applicable rubric could be created similar to the one that was the result of this study. Such a rubric must encompass broader characteristics of predatory practices, including but not limited to publisher website homepage objectives, review process transparency, publication speed, frequency of retracted papers, analysis of author communication, publisher advertising objectives, journal naming conventions, frequency of publisher website updates, and the publisher's intended audience.

We have thus far avoided submission of papers to expected legitimate journals out of ethical concerns. A future experiment that better addresses these concerns is welcomed and we believe necessary to solidify a better rubric, while the goal of this paper is testing the foundational viability of submissions at scale. Future research directed towards creating AI tools that use the developed rubrics to assess the credibility of publishers, or even the efficacy of reviewers by legitimate journals, would be valuable. Leveraging AI to analyze publisher or peer review characteristics would enable authors to make more informed decisions when considering publication opportunities.

Finally, a study tracking the development of predatory publishers' characteristics and tactics over time would be valuable in breaking down their intent and action for further evaluation. Ultimately, by continuing to refine evaluation tools and developing solutions that probe their decisions processes, we can provide authors with the necessary knowledge to mitigate the threat of predatory publishing.

Acknowledgements

This work was sponsored in part by the VTNSI and the Commonwealth Cyber Initiative. The positions, opinions, and viewpoints are those of the authors alone.

References

Jeffrey Beall. 2012. Beall's list of predatory publishers. *Muhammadiyah Sidoarjo University*.

Kirsten Bell. 2017. 'Predatory' open access journals as parody: Exposing the limitations of 'legitimate' academic publishing. *Open Access Jnl for a Global Sustainable Information Society*, 15(2):651–662.

Lizzie Burgiss, Ben Tatum, Christopher Henshaw, Madison Boswell, and Alan J. Michaels. 2024. Github: https://github.com/lizzieburgiss/predatory-publishers-research-apendix.

Companies London. 2024. Companies London: Walsh Medical Media Ltd.

Check Company. 2023. Check company: Free business and director reports.

Andrea Cortegiani and Steven L Shafer. 2018. "Think. Check. Submit." to avoid predatory publishing. *Critical Care*, 22(1):300.

Soumitra Das and Seshadri Chatterjee. 2018. Cabell's blacklist: A new way to tackle predatory journals. *Indian Jnl of Psychological Medicine*, 40(2):197–198.

Datalog. 2023. Datalog Conference Series LLC.

Esme E Deprez and Caroline Chen. 2017. Medical journals have a fake news problem. *Bloomberg*.

Sarah Elaine Eaton. 2018. Avoiding predatory journals and questionable conferences. *the Education Resource Information Center*.

Dan Eskildsen. 2024. Companies House Data: 35 Ruddlesway.

Federal Trade Commission. 2020. FTC.

Laura E Happe. 2020. Distinguishing predatory from reputable publishing practices. *Journal of Managed Care & Specialty Pharmacy*, 26(8):956–960.

Joe Harrison, Joshua Lyons, Lauren Anderson, Lauren Maunder, Paul O'Donnell, Kiernan B. George, and Alan J. Michaels. 2021. Quantifying use and abuse of personal information. In *2021 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pages 1–6.

Endole Insight. 2023. Endole business information.

Stephen Kimotho. 2019. The storm around Beall's list: A review of issues raised by Beall's critics over his criteria of identifying predatory journals and publishers. *African Research Review*, 13(2):1–11.

Christine Laine and Margaret A Winker. 2017. Identifying predatory or pseudo-journals. *Biochemia médica*, 27(2):285–291.

Adam Marcus, et. al. 2024. Retraction Watch.

Alan J. Michaels and Kiernan George. 2021. Use & Abuse of Personal Information. *Blackhat USA 2021*.

Aso S Muhialdeen, et. al. 2023. Kscien's list. *Barw Medical Journal*.

Devin O'Connor. 2023. Macau casinos drop lawsuit against Alvin Chau, Suncity Junket Group. *Casino.org*.

S. Rele, M. Kennedy, and N. Blas. 2017. Journal evaluation tool. *LMU Libarian Publications and Presentations*.

Steve Robert. 2024. LinkedIn Steve Robert.

G. Schlesselman-Tarango. 2024. Predatory publishers & other bad actors. *Grinnell College LibGuides*.

VAT Search. 2022. VAT search scholars central.

Keerthi Talari and Vinod Ravindran. 2023. Predatory journals: how to recognise and keep clear! *Jnl Royal College of Physicians of Edinburgh*, 53(4):232–236.

Paige Thomas. 2022. Enhanced efficiency in sorting: Unveiling the optimized bubble sort algorithm. *Jnl of Robotics and Automation Research*.

OMICS International USA. 2024. LinkedIn OMICS International USA.

Stuart Yeates. 2017. After Beall's 'list of predatory publishers': problems with the list and paths forward. *Research Applications, Information and Library Studies*.