Current Topics

DIGITAL HEALTH

DIGITAL HEALTH
Volume 9: 1–5

DOI: 10.1177/20552076231176654
journals.sagepub.com/home/dhj

Sage

Medical journals and advertiser tracking–Consequences for patients, clinicians, and editors

Ravi Gupta[1,2], Ari B Friedman[3,4,5] and Matthew S McCoy[3,5]

Abstract

Medical journal websites frequently contain tracking code that transfers data about journal readers to third parties. These data give drug, device, and other medical product companies a potentially powerful resource for targeting advertisements and other marketing materials to journal readers based on unique attributes and medical interests that can be inferred from the articles they read. Thus, while editors may strictly regulate the content of advertisements that such companies place in their journals' pages, they simultaneously provide those companies with the means to target readers in other forums, possibly in ways that subvert editorial guidelines. We examine the implications of third-party tracking on medical journal webpages, and recommend actions that publishers, editors, and academic societies can take to curb it.

Keywords

Third-party tracking, digital privacy, medical journals

Submission date: 29 September 2022; Acceptance date: 2 May 2023

Drug and device companies spend upwards of $20 billion a year on advertising targeting health care providers (HCPs).[1] One of the primary ways these companies reach their intended audience is by placing advertisements in professional medical journals. In principle, these advertisements can increase knowledge of new therapeutics and accelerate their appropriate prescribing in specific patient populations. However, such advertising can also harm public health and raise health care costs by generating demand for therapies with limited evidence of efficacy and cost-effectiveness.[2,3]

Medical journal editors recognize the conflict of interest between running lucrative drug and device advertisements and publishing unbiased scientific findings. Accordingly, most follow International Committee of Medical Journal Editors (ICMJE) guidelines, which, among other measures, recommend that journals not carry advertisements for products proven to be harmful to health and that editors have final authority for approving print and online advertisements.[4]

Little attention has been paid, however, to medical journals' role in facilitating targeted advertising to providers and other journal readers, such as patients, once they have left the journal website. Medical journal websites contain third-party trackers that transfer user data to advertisers, data brokers, and social media companies.[5] These companies can use the information gathered on medical journal pages to target advertisements and other marketing material to journal readers based on their unique attributes and inferred medical interests. Thus, while editors may strictly regulate the content of advertisements that drug and device companies place in their journals' pages, they simultaneously provide those companies with the means to target readers in other forums, possibly in ways that subvert

[1]Division of General Internal Medicine, Johns Hopkins University School of Medicine, Baltimore, MD, USA
[2]Department of Health Policy and Management, Bloomberg School of Public Health, Johns Hopkins University, Baltimore, MD, USA
[3]Leonard Davis Institute of Health Economics, University of Pennsylvania, Philadelphia, PA, USA
[4]Department of Emergency Medicine, Perelman School of Medicine, University of Pennsylvania, Philadelphia, PA, USA
[5]Department of Medical Ethics and Health Policy, Perelman School of Medicine, University of Pennsylvania, Philadelphia, PA, USA

Corresponding author:
Ravi Gupta, Johns Hopkins University School of Medicine, Baltimore, MD, USA.
Email: ravigupta@jhmi.edu

ICMJE guidelines. We examine the extent and implications of third-party tracking on medical journal websites and then describe steps that journal editors and publishers can take to protect the privacy of visitors to their websites.

What is third-party tracking?

Third-party trackers are hidden pieces of code embedded on many websites[6–9] that initiate data transfers from a user's computer to third-party domains—that is, entities other than the website the user is visiting. When someone visits HHS.gov, for example, a third-party tracker sends information about that visit to the ad service DoubleClick (owned by Google). These data transfers typically include users' IP address and URLs of visited webpages. Many third parties also set cookies on users' browsers—small pieces of data that serve as persistent identifiers, allowing users to be tracked across multiple websites. Using these tools, companies are able to construct detailed profiles of individuals' browsing behaviors, which can, in turn, be linked to email addresses, social media profiles, and other real-world identifiers.

Third-party tracking on medical journal websites

Because third-party tracking is designed to be invisible to web users, many readers likely have no idea how much tracking they are exposed to when they visit a medical journal website. However, we have found that more than 99% of medical journals with an impact factor of two or greater[8] include at least one third-party tracker on their website.[5] In fact, the average medical journal website had 31 third-party trackers sending data to domains owned by different parent companies. Figure 1 displays the unique third-party tracking entities on two of the top 10 medical journals by impact factor. We also found that six medical journals had no third-party tracking on their websites, suggesting that it is possible for a journal website to serve its primary function—presenting academic articles—without facilitating targeted advertisement to its readers. Journals without tracking had similar impact factors to all studied journals (within the interquartile range), but were from small publishers and had basic websites with less functionality. Future studies could examine in greater depth the properties and policies of medical journal websites that have no third-party tracking.

The most prolific trackers on medical journal websites are operated by familiar big tech companies, including Google/Alphabet, Twitter, and Facebook. While these companies allow advertisers to reach a wide variety of audiences across a vast range of websites, many also support advertisers that seek specifically to target HCPs and patients. Google's advertising policy, for instance, contains guidelines to allow pharmaceutical companies to promote prescription drugs to users whose data they have collected.[10] Adobe and Oracle, each of whose trackers appeared on at least 40% of medical journal websites, have published lists with many medical specialties in the audience "segments" available to direct targeted advertising.[11,12] By selecting among these segments, a pharmaceutical company could, for instance, display advertisements to users inferred to be "addiction medicine" or "child and adolescent psychiatry" providers. These companies also include groups with different health conditions in their audience segments, allowing advertisers to target, for example, individuals who are likely to purchase certain anti-allergy medications. Other companies, like DMD Marketing Corporation, whose trackers appeared on the websites of several leading medical journals, specialize in targeting HCPs,[13] offering pharmaceutical companies the ability to deliver targeted marketing materials "based on an HCP's browsing behavior." They suggest, for instance, that "if an HCP visits the latest clinical trial summary, the system might automatically send an email from the sales rep that contains the full clinical trial report as an attachment."

What are the implications of third-party tracking on medical journals?

The invisible but ubiquitous presence of third-party trackers on medical journal websites gives drug and device companies a particularly powerful tool for advertising to providers based on the journal websites they visit and the articles they read. Trackers can, for example, infer that a visitor to a journal's website is a physician reading about type 2 diabetes treatments and then show that individual an advertisement for a particular company's new diabetes therapy. That advertisement could be displayed on the journal's website if the journal allows for the placement of targeted advertisements, or it could be displayed on a string of other websites visited by the physician. Unlike static advertisements that appear in print or digital versions of medical journals—which frequently do not adhere to FDA safety guidelines[14] but can in principle be monitored by journal editors—there is no reliable mechanism for ensuring that targeted pharmaceutical advertisements shown to physicians on other websites contain adequate safety information or even that they are for products proven to be safe and effective.

Patients who access medical journal websites to learn more about their own health conditions may also be at risk from targeted advertising. An older adult who, following a diagnosis of mild cognitive impairment, starts reading articles and commentaries on Alzheimer's trials may suddenly start receiving targeted advertisements for both legitimate drugs and for unproven therapies. In addition to potentially exposing patients to misleading information, when such advertisements begin appearing on shared computers, they may also compromise patient privacy.[15–17]

Recommendations

Regulatory oversight of third-party tracking varies but is generally minimal. In the U.S., while communication

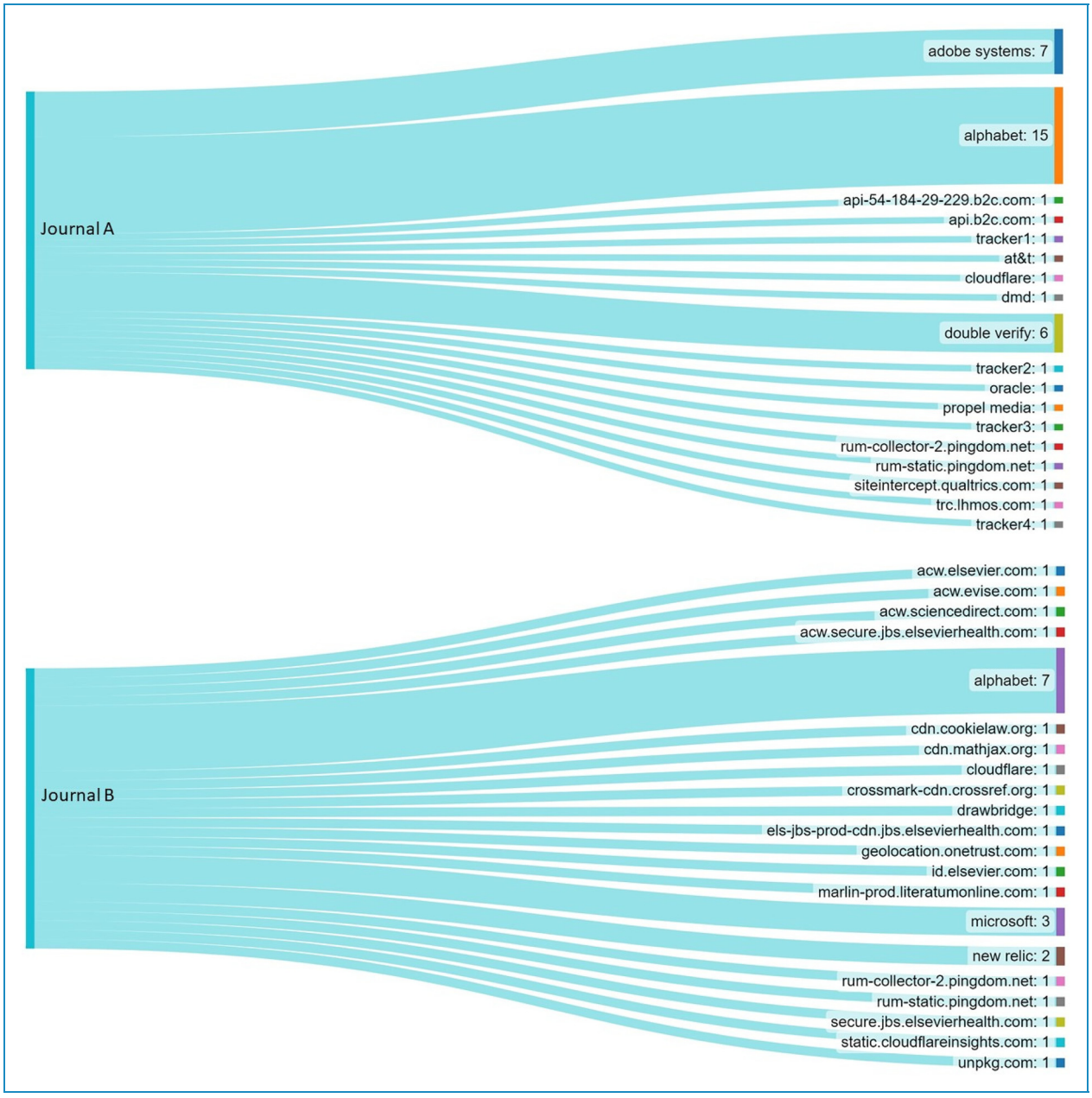

Figure 1. Data transfers to third-party domains on two of the top 10 medical journal websites (by impact factor), by parent company.

between HCPs and patients is protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), no such regulation protects health-related information that can be inferred from web browsing. Attempts at regulating digital privacy and tracking, such as the California Consumer Privacy Act of 2018, have faced substantial legal and technological barriers to successful implementation.[18] In Europe, the General Data Protection Regulation (GDPR), which protects online personal data by informing users of cookies and restricting data collection and use through the levying of penalties, has similarly faced enforcement challenges due to evasion and budgetary constraints.[19] Though GDPR tightened consent rules, consent alone may be insufficient,[20] as users may frequently click through complicated consent banners online and be unaware of profile construction. One issue in particular has been the growing consolidation among firms that engage in third-party tracking.[21] Market concentration enables construction of richer and potentially more sensitive user profiles, which has implications for privacy. In the U.S., greater Federal Trade Commission oversight of digital privacy and anti-trust laws more broadly and health tracking more specifically, as well as continued efforts to enact federal privacy laws, may begin to

address some of the issues of targeted advertising to HCPs through third-party tracking.

Fortunately, journal editors can also take immediate steps to begin shielding readers from third-party tracking. First, using freely available privacy monitoring tools such as OneTrust, TrustArc, and Osano, editors should undertake privacy audits of their websites to make themselves aware of the trackers that are currently present. Some publishers may have simply overlooked the fact that "free" tools used to monitor website traffic and performance also transfer data to third parties, and might be responsive to editor requests to reduce or eliminate unnecessary tracking. With better awareness of the trackers on their websites, editors and publishers will be able to make informed decisions about how to optimize privacy protections on their websites. Second, if they are unwilling or unable to eliminate all trackers in the near term, editors should at least give users the option to limit third-party tracking. Currently, many medical journals deny access to users who take the basic privacy-protecting step of blocking cookies,[22] making privacy-conscious readers choose between foregoing access to journal content and allowing tracking. Instead of compelling this tradeoff, journal websites can and should be modified to allow full access to users blocking cookies. Ultimately, medical journal editors should commit to working with publishers to eliminate third-party trackers on their websites, as a small number of journals have done.[5] Existing ICMJE recommendations prohibit selling advertisements intended to be juxtaposed with journal content on the product being advertised. This norm should be supported by medical professional societies. Notably, these changes would not prohibit journals from running digital advertisements, so long as those advertisements are contextual rather than targeted, with no user data flowing to third parties. In fact, the experience of other online publishers suggests that the switch from targeted to contextual advertising would have minimal impact on journals' advertising revenue.[23]

Conclusion

While many medical journals rely on income from online advertising, they can and should do so without helping advertisers and other third parties accumulate data about their readers. Consistent with their commitment to curbing misleading or harmful advertising, medical journal editors and publishers should work towards ending their participation in the targeted advertising economy.

Acknowledgments: All authors had access to all the study data, take responsibility for the accuracy of the analysis, and had authority over manuscript preparation and the decision to submit the manuscript for publication.

Contributorship: Study concept and design: All authors.
Drafting of manuscript: Gupta and McCoy.
Critical revision of manuscript for important intellectual content: All authors.
Supervision: McCoy and Friedman.

Declaration of conflicting interests: Dr. McCoy is an uncompensated member of the University of Pennsylvania's Data Ethics Working Group, which is funded in part through industry gifts to the university. The authors declare no competing financial or non-financial interests.

Ethical approval: Not applicable.

Funding: The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: Support for this research was provided by the Public Interest Technology University Network Challenge Fund, a fiscally sponsored project of New Venture Fund. The Public Interest Technology University Network's challenge grants are funded through the support of the Ford Foundation, Hewlett Foundation, Mastercard Impact Fund with support from Mastercard Center for Inclusive Growth, Patrick J. McGovern Foundation, the Raikes Foundation, Schmidt Futures, and the Siegel Family Endowment. Penn's Medical Communications Research Institute supported Drs. Friedman and McCoy's effort in preparing this manuscript.

Guarantor: Not applicable.

ORCID iD: Ravi Gupta https://orcid.org/0000-0001-5902-6414

References

1. Schwartz LM and Woloshin S. Medical marketing in the United States, 1997–2016. *JAMA* 2019; 321: 80–96.
2. Sinha MS, Kesselheim AS and Darrow JJ. Pharmaceutical advertising in medical journals: revisiting a long-standing relationship. *Chest* 2018; 153: 9–11.
3. Manz C, Ross JS and Grande D. Marketing to physicians in a digital world. *N Engl J Med* 2014; 371: 1857–1859.
4. International Committee of Medical Journal Editors. Advertising. 2022; https://www.icmje.org/recommendations/browse/publishing-and-editorial-issues/advertising.html. Accessed May 1, 2022.
5. Gupta R, Friedman AB and McCoy MS. Prevalence of third-party tracking on medical journal websites. *JAMA Health Forum* 2022; 3: e220167.
6. Zheutlin AR, Niforatos JD and Sussman JB. Data-tracking on government, non-profit, and commercial health-related websites. *J Gen Intern Med* 2021; 37: 1315–1317.
7. Niforatos JD, Zheutlin AR and Sussman JB. Prevalence of third-party data tracking by US hospital websites. *JAMA Netw Open* 2021; 4: e2126121.
8. McCoy MS, Libert T, Buckler D, et al. Prevalence of third-party tracking on COVID-19-related web pages. *JAMA* 2020; 324: 1462–1464.
9. Friedman AB, Merchant RM, Maley A, et al. Widespread third-party tracking on hospital websites poses privacy risks

for patients and legal liability for hospitals. *Health Aff (Millwood)* 2023; 42: 508–515.
10. Google. Advertising policies help—healthcare and medicines. 2022; https://support.google.com/adspolicy/answer/176031?hl=en#:~:text=Allowed%20with%20limitations-,Google%20doesn't%20allow%20the%20use%20of%20prescription%20drug%20terms,prescription%20drug%20terms%20in%20keywords/. Accessed April 13, 2023.
11. Adobe Inc. Adobe advertising cloud - available third party health segments 2019. 2019; https://web.archive.org/web/20191122182020/https://www.adobe.com/content/dam/acom/en/privacy/pdfs/Adobe-Advertising-Cloud-Health-Segments-2019.pdf. Accessed April 13, 2023.
12. Oracle. Health and wellness preference data segments. 2021; https://www.oracle.com/us/assets/health-wellness-data-segments-2537888.pdf. Accessed April 13, 2023.
13. DMD Connects. HCP audience identity management. 2016; http://media.mmm-online.com/documents/237/dmd_hcp_aim_ebook_59160.pdf. Accessed October 1, 2021.
14. Korenstein D, Keyhani S, Mendelson A, et al. Adherence of pharmaceutical advertisements in medical journals to FDA guidelines and content for safe prescribing. *PLoS One* 2011; 6: e23336.
15. Libert T. Privacy implications of health information seeking on the web. *Commun ACM* 2015; 58: 68–77.
16. Gopal RD, Hidaji H, Patterson RA, et al. Dark clouds and silver linings: impact of COVID-19 on internet users' privacy. *JAMIA Open* 2021; 4: ooab100.
17. Bujlow T, Carela-Espanol V, Sole-Pareta J, et al. A survey on web tracking: mechanisms, implications, and defenses. *Proc IEEE* 2017; 105: 1476–1510.
18. Kaye K. In some California privacy cases, analytics trackers are in the crosshairs—and violators could be charged by the cookie. 2021. Accessed March 29, 2022.
19. Kollnig K, Binns R, Van Kleek M, et al. Before and after GDPR: tracking in mobile apps. *Internet Policy Rev* 2021; 10.
20. Gupta R, Iyengar R, Sharma M, et al. Consumer views on privacy protections and sharing of personal digital health information. *JAMA Netw Open* 2023; 6: e231305.
21. Binns R and Bietti E. Dissolving privacy, one merger at a time: competition, data and third party tracking. *Comput Law Secur Rev* 2020; 36.
22. Friedman AB, Miller E and McCoy MS. Prevalence of medical journal websites that deny access to users who block browser cookies. *JAMA Netw Open* 2021; 4: e213492.
23. Davies J. After GDPR, The New York Times cut off ad exchanges in Europe—and kept growing ad revenue. January 16, 2019; https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/s. Accessed May 10, 2022.