to pay for it.” It seems that many are flying first class when we cannot really afford it.

Although these data demonstrate that endoscopy nurses and physicians prefer propofol, it seems that there is a large difference between actual cost and perceived value.

Deepak Agrawal, MD, MPH
Don C. Rockey, MD

Author Affiliations: Division of Digestive and Liver Diseases, University of Texas Southwestern Medical Center, Dallas (Agrawal); Department of Internal Medicine, Medical University of South Carolina, Charleston (Rockey).

Corresponding Author: Don C. Rockey, MD, Department of Internal Medicine, Medical University of South Carolina, 96 Jonathan Lucas St, Ste 803, Charleston, SC 29425 (rokeye@musc.edu).

Author Contributions: Both authors had full access to all the data in the study and take responsibility for the integrity of the data and the accuracy of the data analysis.

Study concept and design: Both authors.

Acquisition of data: Agrawal.

Analysis and interpretation of data: Both authors.

Drafting of the manuscript: Both authors.

Critical revision of the manuscript for important intellectual content: Both authors.

Statistical analysis: Both authors.

Administrative, technical, and material support: Both authors.

Study supervision: Rockey.


Conflict of Interest Disclosures: None reported.

Additional Contributions: We thank all of those who filled out questionnaires.


Privacy Threats When Seeking Online Health Information

Patients increasingly use the Internet to access health-related information for which they are not charged.1 In turn, websites gather information from those who browse their sites and target advertisements to them. Yet this business model masks a more complicated picture.

A patient who searches on a “free” health-related website for information related to “herpes” should be able to assume that the inquiry is anonymous. If not anonymous, the information knowingly or unknowingly disclosed by the patient should not be divulged to others.

Unfortunately, neither assumption may be true. Anonymity is threatened by the visible Internet address of the patient’s computer or the often unique configuration of the patient’s web browser.2 Confidentiality is threatened by the leakage of information to third parties through code on websites (eg, iframes, conversion pixels, social media plug-ins) or implanted on patients’ computers (eg, cookies, beacons).

Many third parties use the information they collect only to target advertising (eg, DoubleClick). However, nearly 300 third parties use the information to track consumers,3 delivering advertising related more directly to the user's known or inferred interests, demographics, and prior online behavior.

These weaknesses in privacy practices have been detailed in the news media.4 The Federal Trade Commission has called for consumer privacy legislation.5 Online privacy guidelines for searches on health topics have been published.6 But privacy threats are poorly understood because of the technical nature of online data collection and aggregation.

Methods I therefore explored this potential problem between December 2012 and January 2013 using a convenience sample of 20 popular health-related websites. I used freely available privacy tools (DoNotTrackMe [www.abine.com] and Ghostery [www.ghostery.com]) to detect third parties. These tools are downloadable and installed as add-ons to a web browser. I purchased and installed commercial interception software (Charles [www.Charlesproxy.com]) to intercept hidden traffic from my computer to the websites of third parties.4,7 On each site I browsed 10 pages randomly and searched for content related to “depression,” “herpes,” and “cancer.”

Results I found that all 20 sites had at least 1 third-party element, typically 6 or 7. Most of these elements had nontracking functions. Thirteen of the 20 websites had 1 or more tracker elements (Table). Unlike most of the commercial and mass media sites sampled, I found no tracking elements on physician-oriented sites closely coupled to professional groups. Social media networks use plug-in buttons (eg, Facebook’s “Like” button) to allow tracking on websites even if the online user is not logged into social media, and even if the user does not actually press the social button. Five of the 13 sites that had tracker elements had also enabled such social media button tracking.

Using the interception tool, I found that my searches on websites for the 3 terms were leaked to third-party tracking entities by 7 websites. The search terms were not leaked to third-party tracking sites when I browsed US government sites or 4 of the 5 physician-oriented sites.

Discussion In general, the information gathered by websites and their third-party affiliates enhances the online user’s experience and allows targeted advertisements, which support a free business model. However, threats to privacy are real and are insufficiently addressed in current legislation and regulations.3 Were such risks to be realized, the ramifications could span embarrassment, discrimination in the labor market, or the deliberate decision by marketers not to offer or ad-
Table. Tracking of Searches at 20 Health-Related Websites

<table>
<thead>
<tr>
<th>Medical Information Website</th>
<th>Website Contains Third-Party Tracking Elements</th>
<th>Website Leaked Search Terms to Third-Party Tracking Entities</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Institutes of Health</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Food and Drug Administration</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>PubMed</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>MedlinePlus</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Centers for Disease Control and Prevention</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>National Cancer Institute</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>National Health Service UK</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>New England Journal of Medicine</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>JAMA</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>JAMA Internal Medicine</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Medscape</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Medical NewsDaily/Mdlinx</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mayo Clinic</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>WebMD</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Weight Watchers</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Drugs.com</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Men’s Health</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Health.com</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Fox News: Health</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>New York Times: Health News</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

* Tracking refers to the ability of third-party affiliates of a website to track users. A tracking element is a long-acting cookie, web beacon, conversion pixel, social media tracking plug-in, or other script that reports to a third party about the user’s online behavior at current or subsequent sites. I identified these by using DNTMe (www.abine.com) and Ghostery (www.evidon.com), which are both free software add-ons.

leakage refers to the sharing of a user’s search terms with third parties. I conducted searches while on each website for “herpes,” “depression,” and “cancer.” I identified leakage by using Charles, a commercially available interception software (www.charlesproxy.com), to directly monitor internet communication between my computer and any third parties.

vertise particular goods and services to an individual, based solely on the companies’ privately gathered knowledge.

I could not determine whether leaked information was used or misused by third parties. However, the leakage of search terms to tracking entities is worrisome. All the websites I reviewed have privacy protection statements. The alert users to data sharing and undertake to protect individual data through contractual agreements that mandate aggregation and deidentification of user data. Nevertheless, such agreements are generally not disclosed to users and may not survive a change of corporate ownership. Commercial websites may also disclose user activity to the government, as recent National Security Agency news stories have suggested.

Security concerns about health care information have traditionally revolved around the loss or theft of patient information from health care provider health records or the misuse of information by health care providers. Yet much health-related information is not stored in electronic health records, but generated in private health-related searches.

My findings suggest that patients and physicians who are concerned about the privacy of information about their health-related searches may prefer to search through government websites or those of professional societies. Alternatively, individuals can use privacy tools that are available free of charge when searching and browsing online. Examples are DoNotTrackMe and Ghostery. Use of these tools created some inconveniences but generally did not affect the functionality of the websites I examined.

Failure to address these concerns may diminish trust in health-related websites and reduce the willingness of some people to access health-related information online. Until strong consumer privacy legislation is enacted, individuals should take care how much trust they place in their anonymity and the confidentiality of their information when online.

Marco D. Huesch, MBBS, PhD

Author Affiliations: Sol Price School of Public Policy, University of Southern California, Los Angeles; Leonard D. Schaeffer Center for Health Policy and Economics, University of Southern California, Los Angeles; Department of Community and Family Medicine, Duke University School of Medicine, Durham, North Carolina; Department of Health Sector Management Area, Duke University Fuqua School of Business, Durham, North Carolina.

Corresponding Author: Marco D. Huesch, MBBS, PhD, USC Price School of Public Policy, Gateway–Unit A, 3335 S Figueora St, Los Angeles, CA 90089-7273 (huesch@usc.edu).

Published Online: July 8, 2013. doi:10.1001/jamainternmed.2013.7795.

Conflict of Interest Disclosures: Dr Huesch receives salary, research, and travel support from the Agency for Healthcare Research and Quality (R21 HS021868-01) for a social media and Internet-based project, and from Lockheed Martin for a project, both not related to this study. Dr Huesch also reports receiving payments for consulting to the Institute of Medicine and manuscript preparation unrelated to this study from Precision Health Economics, a pharmaceutical consultancy.

Disclaimer: This study was not reviewed by funders’ representatives and does not reflect their official positions.


