Original Manuscript

Addressing Online Health Privacy Risks for Older Adults: A Perspective on Ethical Considerations and Recommendations

Gerontology & Geriatric Medicine
Volume 8: 1–7

DOI: 10.1177/23337214221095705
journals.sagepub.com/home/ggm
SAGE

Ari B. Friedman, MD, PhD[1,2], Chris Pathmanabhan, MBE[1], Allen Glicksman, PhD[3], George Demiris, PhD[4], Anne R. Cappola, MD, ScM[1], and Matthew S. McCoy, PhD[1]

Abstract

The rise in online health information seeking among older adults promises significant benefits but also presents potentially serious privacy risks. In light of these risks, we argue that ongoing research and advocacy aimed at promoting online health information seeking among older adults must be coupled with efforts to identify and address threats to their online privacy. We first detail how internet users reveal sensitive health information to third parties through seemingly innocuous web browsing. We then describe ethical concerns raised by the inadvertent disclosure of health information, which include the potential for dignitary harms, subjective injuries, online health scams, and discrimination. After reviewing ways in which existing privacy laws fail to meet the needs of older adults, we provide recommendations for individual and collective action to protect the online privacy of older adults.

Keywords

bioethics, life expectancy/longevity, digital health, health privacy

Manuscript received: January 9, 2022; **final revision received:** March 8, 2022; **accepted:** April 4, 2022.

Impact Statement

We certify that this work is novel. The rise in online health information seeking among older adults promises significant benefits but also presents potentially serious privacy risks. This article details how internet users can reveal sensitive health information via web browsing, describes relevant ethical concerns, which include the potential for dignitary harms, subjective injuries, online health scams, and discrimination.

Key Points

- 75% of adults 65+ use the internet, frequently for medical advice.
- Online browsing can reveal more about your health than a smart scale or fitness tracker, yet is poorly regulated.
- Older adults face increased and unique privacy risks and merit additional guidance and regulatory protection.

Why Does This Matter?

Older patients and those who advise them should takes steps to limit privacy invasions and health tracking and advocate for more protective policies.

[1]Perelman School of Medicine, University of Pennsylvania, Philadelphia, PA, USA
[2]Leonard Davis Institute of Health Economics, University of Pennsylvania, Philadelphia, PA, USA
[3]Research Department, New Courtland, Philadelphia, PA, USA
[4]School of Nursing, University of Pennsylvania, Philadelphia, PA, USA

Corresponding Author:
Ari B. Friedman, Department of Emergency Medicine, Perelman School of Medicine, University of Pennsylvania, 3400 Civic Center Boulevard, Philadelphia, PA 19104, USA.
Email: arib@alumni.upenn.edu

Introduction

Over the past two decades, the internet has transformed how older adults access health information (Waterworth & Honey, 2018). In 2000, just 14% of adults aged 65 and up reported using the internet. By 2021, the number had climbed to 75% (Pew Research Center, 2021). Among the growing number of older adults who use the internet, health information seeking is the third most popular online activity, trailing only email use and general information searches (Berkowsky & Czaja, 2018). Additionally, despite some concerns about the trustworthiness of online health information, older adults who use the internet rank it as their third most preferred source of health information, "behind only health care providers and pharmacists" (Berkowsky & Czaja, 2018).

The rise in online health information seeking among older adults promises significant benefits. Online health resources "can be a gateway to meet the healthcare needs of a growing older population…particularly for those living in isolated rural communities" (Waterworth & Honey, 2018). Internet use can also foster patient empowerment by connecting older adults with others facing common health challenges and providing "information about health, wellness, and healthcare," which allows them "to take a more active role in managing their health" (Berkowsky & Czaja, 2018).

But along with these benefits come potentially serious privacy risks (Libert et al., 2015; McCoy et al., 2020). Over 90% of health-related web pages contain code that initiates data transfers to third parties (Libert, 2015). Known as "web tracking," this practice effectively shares users' browsing histories with advertisers, data brokers, and other companies that seek to profit from it. Subject to minimal legal regulation, the companies that collect this data are free to sell it or use it for a variety of purposes, including targeting advertisements for both legitimate and sham medical products to users based on their inferred health conditions and concerns (Libert, 2015). This targeted advertising may provide some benefits in the form of offering health-improving products and services to individuals. However, the ubiquitous and unregulated nature of the data marketplace also brings the potential for significant harms.

While older adults are not the only group tracked online, they may be at increased risk of harms associated with web tracking. As a group, older adults have significant health needs and concerns (Salive, 2013) and often considerable spending power (Bhutta et al., 2020). Some have increased susceptibility to deceptive marketing due to cognitive aging and Alzheimer's Disease and Related Diseases (ADRD) (Han et al., 2015). These characteristics make older adults particularly attractive targets for online health scams (James et al., 2014). Additionally, while there is limited data regarding older adults' facility with tools to protect their online privacy, such as browser extensions and ad blockers, they generally appear to adopt fewer privacy protection technologies (Van den Broeck et al., 2015). The ability to protect one's privacy online also seems to be lower among individuals with lower technological literacy, suggesting that disadvantaged older adults may be at highest risk of privacy-related harms (Baruh et al., 2017).

In light of these risks, ongoing research and advocacy aimed at promoting online health information seeking among older adults must be coupled with efforts to identify and address threats to their online privacy. While such efforts are ethically justified as a means of preventing harm, they may have the additional instrumental benefit of promoting older adults' effective use of online health resources including, increasingly, telehealth. Older adults have identified privacy concerns as one of the primary barriers to their adoption of new technologies (Baig, 2021). Thus, taking steps to address these concerns may lower this critical barrier to adoption.

In what follows, we detail how internet users can inadvertently reveal sensitive health information to third parties and explain why this raises particular ethical concerns for older adults. We then show why current laws and regulations offer inadequate protections against these risks, especially for older adults who may lack the knowledge and technical literacy to read through dense privacy policies and exercise opt-out rights granted by recent privacy laws. Given these challenges, we argue that older adults can take meaningful steps to protect themselves from privacy-related risks by adopting safer online privacy behaviors. Those who support older adults—including caregivers, non-profits, social service agencies, educational institutions, and clinicians—can help older adults' protect their health privacy by assisting them in adopting these solutions.

How Online Activity Reveals Health Information

Compared to smarthome devices, wearables, and other technologies used to monitor the health and functioning of older adults, browsing activity may seem like an unlikely source of sensitive health information. In reality, however, the websites that people visit can reveal just as much about their health status as the output of their digital scales or sleep trackers.

Several factors combine to make online activity a particularly revealing source of health information. The first is the ubiquity of tracking on health-related web pages. A 2015 study of over 80,000 health-related web pages found that 91% initiated data transfers to third parties, while 71% used third-party cookies—data stored on a user's computer that can serve as a persistent identifier to facilitate the tracking of individuals across multiple websites (Libert et al., 2015). The pervasiveness of tracking across health-related web pages means that almost every time someone visits a web page to read about cancer, ADRD, or another condition, that visit is logged by third parties who can use the information to build detailed profiles of internet users' interests in particular health conditions (Figure 1).

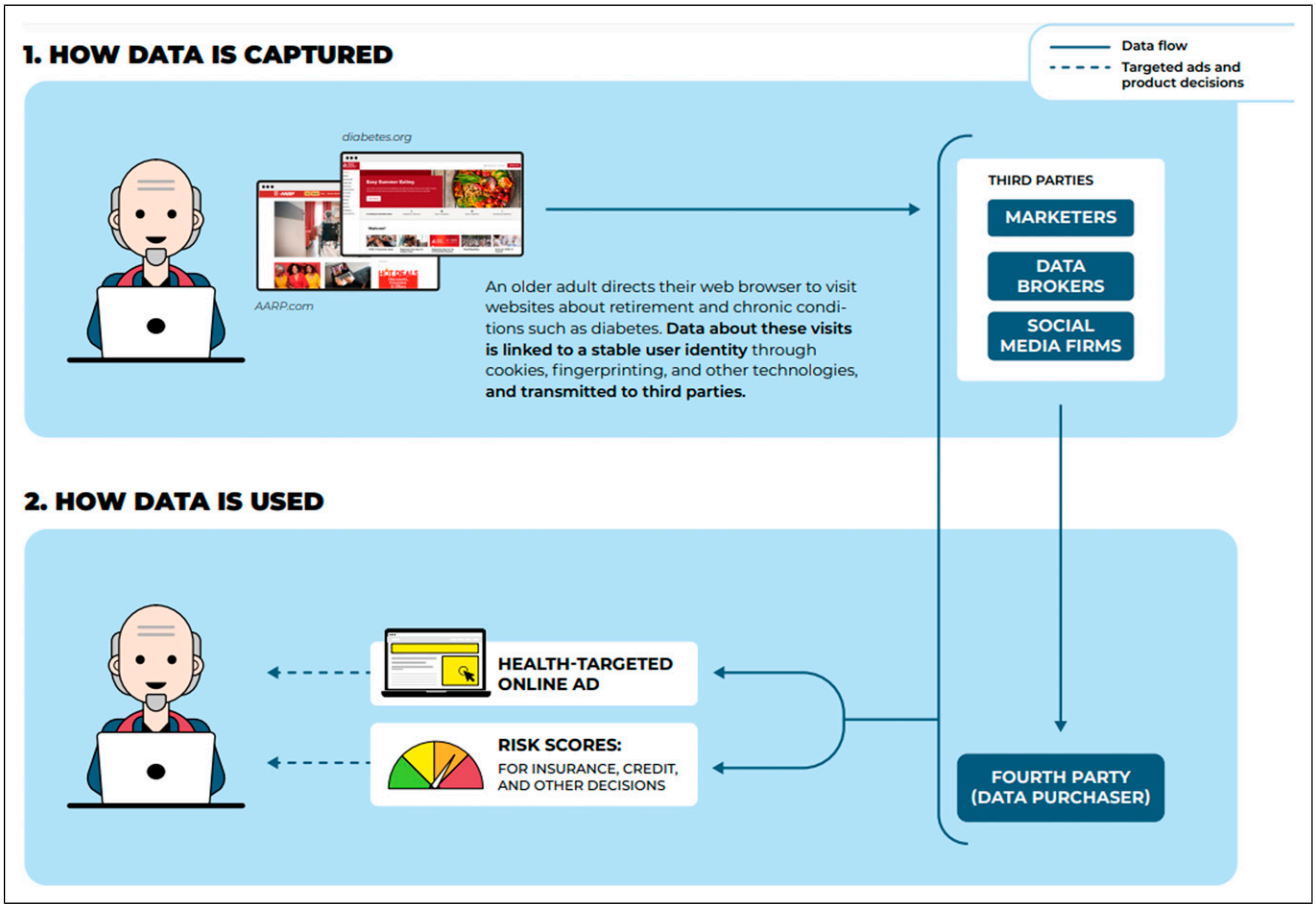

Figure 1. Schematic representation of health profiling from online browsing habits of older adults.

Second, these browsing histories can be readily linked with other forms of data, including purchase histories, publically available data sets, and even personally identifiable information such as names and email address. This allows third parties to link users' health-related web searches and site visits with their real world identities to produce a kind of "shadow health record" (Price et al., 2019). Indeed, in 2015, investigative journalists were able to use a data broker to purchase the names, addresses, ages, and email addresses of 500 individuals believed to have diabetes and 500 individual believed to have asthma (6abc Philadelphia, 2015). The dataset, which cost only $500, also included individuals' incomes, their number of children, and their children's ages.

Third, machine learning algorithms can link health-related web browsing and a targeted outcome, such as the purchase of a medical product, to make predictions based on an individual's past behavior or similar individuals' behavior. In clinical medicine, logistic regression models developed to fit research databases can predict post-operative mortality even for older patients who did not participate in the study by using covariates in common between the patients studied and the patients the tool is later used with (Robinson et al., 2009). Similarly, machine learning models can predict health-related purchasing behavior or disease diagnoses even if that individual has not contributed any outcome data to the third-party database (Kuhn & Johnson, 2013).

Finally, because much browsing data is retained permanently, health-related inferences accumulate across patients' aging trajectories, providing not just a snapshot, but a dynamic record of changing health needs. For instance, a healthy 65-year-old adult with mild osteoporosis might search for retirement advice, revealing their approximate age (Goel et al., 2012). This may give way to searches for active vacations involving significant walking, indicating they have few limitations of instrumental activities of daily living (IADL) (Martin et al., 2017). As IADL deficits accumulate, the same individual, now in their 70's, may search for cruises and mobility assistance devices, giving advertisers clues as to the patient's changing physical health status (Martin et al., 2017). Later searches for incontinence management products after a hospitalization from a fall and hip fracture inform advertisers that deficits in activities of daily living (ADLs) have begun accumulating.

Ethical Concerns

Health-related web tracking raises a range of ethical concerns, many of which are particularly acute for older adults.

First, regardless of its material consequences, the unintended and unwanted disclosure of sensitive health information may result in "dignitary harms" (Price & Cohen, 2019). Bioethicists have argued that "in order to live a flourishing life, it is important that there be a part of an individual's life that is his or hers alone, that remains unknown to others unless shared" (Price & Cohen, 2019). Thus, when third parties gain access to sensitive information that an individual would not wish shared, it may constitute a violation of that individual's dignity even if he or she does not suffer any additional ill effects. For example, the mere fact that data brokers compiled and sold lists of individuals with classifications such as "erectile dysfunction sufferers" and "alcoholism sufferers" arguably violated the dignity of those individuals regardless of whether it led them to experience financial loss, discrimination, or other negative consequences (Libert, 2015). While older adults are by no means the only group vulnerable to such dignitary harms, they tend to have greater health needs and concerns than younger groups and thus may be more likely to reveal health information through their online activity (Salive, 2013).

Unwanted disclosure of sensitive health information may also result in "subjective injuries" like shame or embarrassment (Price et al., 2019). Similar to dignitary harms, subjective injuries are not limited to older adults, but the fact that older adults are often more concerned about disclosing personal information suggests that they may be more likely to experience emotional distress as a result of unwanted disclosure (Auxier et al., 2019).

Other ethical concerns stem from third parties' use of tracking information.

Health-related tracking data allows marketers to target advertisements and offers to individuals on the basis of health conditions or concerns that can be inferred from their online activity, even if that activity is seemingly unrelated to health. For example, if individuals who read news articles on Regis Philbin's death tend to click on advertisements for assisted living facilities, then someone who visits such a page will be targeted with those advertisements. Some portion of targeted health-related advertising may be benign or even useful if it alerts users to beneficial health care products. However, health-related tracking data can also be used to push sham medical products and "miracle" cures to consumers. Cognitive aging and ADRD may make some older adults particularly susceptible to deceptive advertising that leverages personal information gleaned from their online activity. In 2020 alone, the Federal Trade Commission (FTC) filed ten actions against companies that deceptively marketed products claiming to cure or treat medical conditions affecting older adults. In addition to harming older adults by offering false hope and possibly substituting for or delaying curative measures, these products can be financially costly (Hall, 2012). One company cited by the FTC, for example, promoted and sold herbal supplements as treatments for cancer and Parkinson's disease at costs of up to $200,000.

Marketers can also use personal data to discriminate against older adults (Libert, 2015; Libert et al., 2015). Information about spending ability, which can be inferred from internet users' browsing, allows marketers to exclude lower-income older adults from certain deals while charging higher prices to higher-income older adults. Additionally, price discrimination—that is, charging different consumers different prices for the same product or service based on their ability to pay—informed by online browsing histories has become routine (Zuiderveen Borgesius & Poort, 2017), and may particularly affect older adults with multiple chronic conditions who are less price sensitive. For instance, ride-share services use the interaction between an individual's history, demographic characteristics, and location data to set pricing (Pattnaik, 2020). Therefore they might charge more for a ride to a geriatrician's appointment for an older adult than for a visit to the same medical building address for a young adult, because the algorithm infers that the older adult has fewer alternative transportation options (Zuiderveen Borgesius & Poort, 2017).

Health-related web tracking may also lead to broader discrimination against older adults. Many companies engaged in health-related web tracking act as data brokers, linking personal information from a variety of sources including web browsing and social media to create detailed personal profiles. These profiles can classify individuals' credit worthiness or eligibility for employment (Smith et al., 2018). This sort of algorithmic risk scoring has been shown to discriminate against minority prospective home buyers and female job applicants (Smith et al., 2018). Given ageism in other settings (Chang et al., 2020), machine learning algorithms may already embed society's biases towards older adults in their risk scoring based on information gleaned from online browsing activity.

Current Regulatory Environment

Both longstanding data protection laws specific to the health sector and more recent general data protection laws fail adequately to address the online privacy risks faced by older adults.

The 1996 Health Insurance Portability and Accountability Act (HIPAA) established standards to protect health data. However, the law applies only to select organizations and individuals that provide health-specific services, such as physicians, hospitals, and insurers. The 2009 Health Information Technology for Economic and Clinical Health Act (HITECH) extended these rules to certain business associates of organizations subject to HIPAA. Even with this extension, however, much health-related data generated outside of clinical encounters, including data from online health information seeking or product purchases, do not receive HIPAA/HITECH protection (Price & Cohen, 2019).

Table 1. Steps Older Adults Can Take to Limit Inadvertent Health-Related Data Sharing With Online Marketers and Data Brokers.

Use a password manager
✓ Have a unique, secure password for every website
✓ Enable two-factor authentication (https://twofactorauth.org)
✓ Consider giving a trusted loved one or caregiver the password manager's overall password in a secured fashion in the will
Manually opt out of data collection on websites (https://simpleoptout.com/)
Use browser add-ons designed to block ads (e.g. uBlock Origin or AdBlock Plus) and tracking (e.g. Ghostery or Privacy Badger)
Choose a privacy-focused browser with up-to-date protections and configure it properly
✓ Enable automatic updates for operating system and web browser
✓ Set DuckDuckGo or IXQuick to be the default browser search engine
✓ Configure cookies to clear each time the browser loads
Practice safer browsing
✓ Do not install further browser add-ons or toolbars without getting advice first
✓ Use Private Browsing or Incognito mode when possible, especially when visiting disease-specific websites
Take individual protective behaviors to limit scams
✓ Do not open e-mail attachments or click on links from strangers, or forwarded from friends that did not originate with the friend
✓ Discuss any concerns about potential scams with trusted family, friends, clinicians, or social resource workers
✓ Resist the pressure to act quickly
Seek out local technology education resources for further education and guidance

Outside of the health domain, several general data privacy laws have been enacted in recent years. While these laws extend consumers' rights over how their data is collected and processed, they have limitations which are particularly relevant for older adults. For example, both the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) grant consumers a right know how data processors are collecting and using their data. In principle, this allows consumers to make informed choices about the entities with which they chose to interact. In reality, however, GDPR- and CCPA-compliant privacy statements can be long, dense, and difficult for users to read or understand (van Ooijen & Vrabec, 2019). Especially for those with limited technological literacy, such privacy statements are hardly sufficient for ensuring informed consent to the collection and use of personal data.

New comprehensive privacy laws also give consumers the right to opt-out of certain data practices. For examples, the CCPA gives Californians the right to ask companies to see what data has been collected on them, to not sell their data, and to delete their personal data. But exercising these opt-out rights requires engaging in "slow, confusing, [and] frustrating" processes (Waddell, 2021). Individuals must go to each company that collects their data directly and follow a different, non-transparent process at each company that often requires disclosing sensitive information, such as government ID photos, birth dates, and social security numbers.

In addition to imposing a time cost, the cognitive effort required to read privacy statements and exercise privacy rights on each website visited in a day may be prohibitive, particularly for older adults with cognitive aging or ADRD. Corporations have taken advantage of cognitive biases to reduce consumers' ability to consent through presenting many choices, defaulting to privacy-minimizing settings, framing that emphasizes the current harms of opting out over the future benefits to privacy, using difficult language, hiding privacy-preserving choices, and requiring registration to access privacy options (Waldman, 2020).

Ultimately, then, despite granting consumers new rights over their data, these regulations burden consumers with taking active steps to protect their online privacy, and with few exceptions allow corporations to design the choice architecture to make exercising those rights difficult.

Recommendations

Complete elimination of threats to health privacy from online tracking is attainable only through comprehensive legislation and robust regulation (Libert, 2015; Libert et al., 2015). However, it is possible to mitigate online privacy risks through individual protective behaviors.

There are several steps older adults can take to limit tracking (Table 1). Browser extensions known as ad blockers and tracking blockers not only eliminate the visual distraction of ads but can staunch the flow of data to third-parties and eliminate the possibility of being lured towards ineffective health measures or health disinformation. Users can use a password manager to generate and remember unique passwords for each account, thereby avoiding using the same password or login information for every account. They can elect to limit data sharing on major websites, including Amazon, Facebook, and Google, by following the links and instructions provided by the Simple Opt Out project (https://simpleoptout.com/).

Individuals should use a browser that offers up-to-date privacy protections, including anti-fingerprinting techniques (e.g. Mozilla's Firefox and Apple's Safari browser).

Browsers, phones, and other electronic devices should be set to auto-update to increase security and to reduce the cognitive burden of dialogs asking to update their devices.

Many older adults have high levels of technological literacy, and will be able to implement these changes for themselves and educate others of their generation and of younger generations. Other older adults will have difficulty implementing these interventions themselves. Some of these older adults with technological dependency will have caregivers who can help them take protective steps. For others, social service agencies can advise and assist older adults on taking effective measures to protect their online health privacy. Even clinicians with limited technological expertise and time can play a key role by screening for high-risk online privacy behaviors and referring their patients to local support agencies who provide instruction and help setting up devices to limit health information sharing during routine web browsing. Receiving assistance is feasible because many of the basic steps an individual can take to limit online data sharing only require taking action once, although ongoing caution will yield further improvements in privacy.

Older adults with interest in taking ongoing action should seek out further education. Computer training in a senior center, library, or similar setting can not only provide privacy education, but also guidance around what sites are appropriate for learning about specific health conditions in a longitudinal setting. Training in these environments provides an additional opportunity and less pressured environment in which to discuss concerns about literacy and health literacy, which may also improve the quality of health information delivered and provide a trusted advisor to help screen for health scams when targeting does result.

Finally, older adults and their advocates such as professional societies and the AARP should contribute to ongoing debates about comprehensive privacy legislation to ensure that legislative proposals reflect the particular needs of older adults. For example, individuals should have access to simple, default privacy settings that are recognized and honored across platforms to avoid burdening cognition and allow decisions to be made in a supported setting with family and caregivers. In addition, users should be able to assign their power of attorney decision-making rights over their online privacy, such as the right to delete collected data. Advocates should push for continued regulation of what health-related data is allowed to enter insurance coverage, plan, and premium pricing decisions in Medicare Advantage, as well as expanded protections for health information generated outside of clinical encounters. As for snake oil products and health-related scams, aggressive FTC policing can discourage deceptive marketing. Finally, accessible educational material needs to be developed to increase digital literacy for older adults who may have limited experience with online technologies and find it challenging to navigate the online world without any familiarity with digital terms and concepts.

Conclusion

While online health information seeking can greatly benefit older adults, it can also erode personal privacy. Older adults and those who support them should navigate privacy risks through the adoption of simple and effective measures to protect their personal information, and advocate to ensure that emerging legislative proposals are informed by the needs of older adults.

Declaration of conflicting interests

The author(s) declared the following potential conflicts of interest with respect to the research, authorship, and/or publication of this article: McCoy is an uncompensated member of the University of Pennsylvania's Data Ethics Working group, which is funded in part by industry gifts to the university.

Funding

The author(s) 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.

ORCID iDs

Ari B. Friedman https://orcid.org/0000-0003-0412-6754
Allen Glicksman https://orcid.org/0000-0001-7867-6666
Matthew S. McCoy https://orcid.org/0000-0002-5273-3877

References

6abc Philadelphia. (2015, May 10). *Your health info may be bought and sold online*. https://6abc.com/695888/

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Baig, E. (2021). *Older adults wary about their privacy online*. AARP. https://www.aarp.org/home-family/personal-technology/info-2021/companies-address-online-privacy-concerns.html

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26–53. https://doi.org/10/f9zfcf

Berkowsky, R. W., & Czaja, S. J. (2018). 2—Challenges associated with online health information seeking among older adults. In R. Pak, & A. C. McLaughlin (Eds.), *Aging, technology and health* (pp. 31–48). Academic Press. https://doi.org/10.1016/B978-0-12-811272-4.00002-6

Bhutta, N., Bricker, J., Chang, A. C., Dettling, L. J., Goodman, S., Moore, K. B., Reber, S., Volz, A. H., & Windle, R. A. (2020). *Changes in U.S. family finances from 2016 to 2019: Evidence from the survey of Consumer finances* (p. 42). Board of Governors of the Federal Reserve System.

Chang, E.-S., Kannoth, S., Levy, S., Wang, S.-Y., Lee, J. E., & Levy, B. R. (2020). Global reach of ageism on older persons' health: A systematic review. *PLoS One*, *15*(1), Article e0220857. https://doi.org/10/gh2g5h

Goel, S., Hofman, J., & Sirer, M. (2012). Who does what on the web: A large-scale study of browsing behavior. *Proceedings of the International AAAI Conference on Web and Social Media*, *6*(1), 130–137. https://ojs.aaai.org/index.php/ICWSM/article/view/14266

Hall, H. A. (2012). CAM for cancer: Preying on desperate people? *Progress in Palliative Care*, *20*(5), 295–299. https://doi.org/10/ggsqgr

Han, S. D., Boyle, P. A., James, B. D., Yu, L., & Bennett, D. A. (2015). Mild cognitive impairment and susceptibility to scams in old age. *Journal of Alzheimer's Disease: JAD*, *49*(3), 845–851. https://doi.org/10/f74g5n

James, B. D., Boyle, P. A., & Bennett, D. A. (2014). Correlates of susceptibility to scams in older adults without dementia. *Journal of Elder Abuse & Neglect*, *26*(2), 107–122. https://doi.org/10/gfgzb9

Kuhn, M., & Johnson, K. (2013). *Applied predictive modeling*. Springer Science & Business Media.

Libert, T. (2015). Privacy implications of health information seeking on the web. *Communications of the ACM*, *58*(3), 68–77. https://doi.org/10/gdxwjm

Libert, T., Grande, D., & Asch, D. A. (2015). What web browsing reveals about your health. *BMJ*, *351*(5), h5974–h5974. https://doi.org/10/ggxxmc

Martin, L. G., Zimmer, Z., & Lee, J. (2017). Foundations of activity of daily living trajectories of older Americans. *The Journals of Gerontology. Series B, Psychological Sciences and Social Sciences*, *72*(1), 129–139. https://doi.org/10/gbmkjs

McCoy, M. S., Libert, T., Buckler, D., Grande, D. T., & Friedman, A. B. (2020). Prevalence of third-party tracking on COVID-19–related web pages. *JAMA*, *324*(14), 1462. https://doi.org/10.1001/jama.2020.16178

Pattnaik, A. (2020). How does Uber do Surge Pricing using Location Data? *Locale.ai*. https://blog.locale.ai/how-does-uber-do-surge-pricing-using-location-data/

Pew Research Center: Internet, Science & Tech. (2021). *Internet/Broadband Fact sheet*. https://www.pewresearch.org/internet/fact-sheet/internet-broadband/

Price, W. N., & Cohen, I. G. (2019). Privacy in the age of medical big data. *Nature Medicine*, *25*(1), 37–43. https://doi.org/10/gftqx9

Price, W. N., Kaminski, M. E., Minssen, T., & Spector-Bagdady, K. (2019). Shadow health records meet new data privacy laws. *Science*, *363*(6426), 448–450. https://doi.org/10/gjc944

Robinson, T. N., Eiseman, B., Wallace, J. I., Church, S. D., McFann, K. K., Pfister, S. M., Sharp, T. J., & Moss, M. (2009). Redefining geriatric preoperative assessment using frailty, disability and co-morbidity. *Annals of Surgery*, *250*(3), 449–455. https://doi.org/10/b7knbf

Salive, M. E. (2013). Multimorbidity in older adults. *Epidemiologic Reviews*, *35*(1), 75–83. https://doi.org/10/f4q6gw

Smith, G., Smith, G., & Smith, G. (2018). *High-tech redlining: AI is quietly upgrading institutional racism*. Fast Company. https://www.fastcompany.com/90269688/high-tech-redlining-ai-is-quietly-upgrading-institutional-racism

Van den Broeck, E., Poels, K., & Walrave, M. (2015). Older and wiser? Facebook use, privacy concern, and privacy protection in the life stages of emerging, young, and middle adulthood. *Social Media + Society*, *1*(2), 205630511561614. https://doi.org/10/gj47rz

van Ooijen, I., & Vrabec, H. U. (2019). Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. *Journal of Consumer Policy*, *42*(1), 91–107. https://doi.org/10/ghjpw8

Waddell, K. (2021). *California's new privacy rights are tough to use, consumer reports study finds*. Consumer Reports. https://www.consumerreports.org/privacy/californias-new-privacy-rights-are-tough-to-use/

Waldman, A. E. (2020). Cognitive biases, dark patterns, and the "privacy paradox". *Current Opinion in Psychology*, *31*, 105–109. https://doi.org/10.1016/j.copsyc.2019.08.025

Waterworth, S., & Honey, M. (2018). On-line health seeking activity of older adults: An integrative review of the literature. *Geriatric Nursing*, *39*(3), 310–317. https://doi.org/10.1016/j.gerinurse.2017.10.016

Zuiderveen Borgesius, F., & Poort, J. (2017). Online price discrimination and EU data privacy law. *Journal of Consumer Policy*, *40*(3), 347–366. https://doi.org/10.1007/s10603-017-9354-z