**The Dangers of Tracking and Advertising to our Safety and Personal Information**

Internet tracking is the analysis of online users’ behaviors for the purpose of delivering a more personalized browsing experience [1]. Internet tracking is especially popular for companies who earn most of their revenue from targeted advertisements. Based on the user’s information, purchase/search history or interests, they advertise products they think would be the most enticing to the user. It is important to note that website tracking itself is not illegal [1], but problems arise when most users are blindsided by exactly how their information is being collected and used. The ignorance of users and freedom of websites to collect said information raises many security and privacy concerns of online tracking and advertising [1].

Online advertising has become a major revenue stream for most companies in the current century. The internet advertising market has grown more than 100 times in the last 20 years and is expected to reach $517 billion by the end of 2023 [2]. Companies can now rely on both social media and websites to collect information and promote their businesses [2]. Companies usually operate as third-party hosts where they host advertisements received from ad networks or directly from advertisers [3]. For example, websites like blogs or social networking websites do not directly charge their users money, but still make a profit by hosting ads promoting another company’s products [3]. These blogs and social media platforms prefer to keep their websites free in order to keep user engagement high [3].

In order to present the most enticing ads to us, websites track us via cookies, web beacons and browser finger printing [1]. Most online advertisements use tracking cookies to help identify users and deliver targeted advertising by tracking a user’s movements on the website [3]. For example, Google, a major playing in ad networking companies, uses cookies to deliver ads that are relevant to the user’s interests, control the number of times the user sees a given ad and “measures the effectiveness of ad campaigns” [Google Policies & Principles, 2012].

However, one major problem with the use of tracking cookies is that anonymity amongst users is lost [3]. When a user visits multiple websites on the same ad provider, example Google, the same cookies are used each time [3]. This means that the ad provider is able to track the user’s activity on numerous sites just by compiling the information via tracking the cookies without the user’s knowledge [3]. This poses a serious threat to information security and raises numerous privacy concerns as a host of information is being collected and compiled on the user. Although ad networks are expected to adhere to the privacy act and use collected information only for marketing purposes, users have no power or knowledge regarding what it is actually used for [3]. The collection and storage of information via cookies also gives cybercriminals an opportunity to steal your private information. They could access data broker sites which house your personal information to be used for the personalized ads, and instead peddle false advertisements to you containing malware [1]. This is known as malvertising [1].

Despite decades of security concerns, governments and regulatory agencies have only recently started to take users’ privacy concerns seriously. A Wall Street Journal’s investigation in 2010 exposed just how critical users’ privacy concerns were when they uncovered a host of websites using cookies and surveillance technologies with real time tracking and deactivation resistance being used to continuously monitor and collect users’ information [3]. This continuous monitoring, collecting, and selling of information is so vital to revenue generation for companies that if the government started protecting people’s right to online privacy, the economy would more than likely regress [3]. Due to massive revenue generation by misuse of users’ data, the top priority of a company is never to protect a user’s private information.

Despite the popularity of targeted ads, it is still up to the consumer whether they want to engage with these ads or not. A study done by Alexander Bleier et al [5] shows that the effectiveness of retargeting is heavily influenced by the consumer’s trust in the company [5]. When ads are too close to a consumer’s search and/purchasing history, they tend to feel manipulated or deprived of their freedom of choice [5]. The feeling of being constantly targeted, monitored and having your information analyzed makes consumers less likely to engage with these ads and instead creates feelings of exploitation. A different study done by Angelia et al [4] highlighted that when websites gave users more control or perceived control over their privacy settings, consumers were almost twice as likely to click on personalized ads.

In an attempt to improve consumer privacy and curb tracking and data collection, well-known companies like Apple and Google are developing methods to help restrict the transfer of users’ personal data [2]. In 2017, Apple introduced Intelligent Tracking Prevention (ITP) which helps to protect and improve the privacy of Safari browser users [2]. This includes the ability to delete cookies after 24 hours and automatically clear storage after one week [3]. This helps to protect user privacy since deleting cookies and clearing storage reduces the likelihood of personalized data being analyzed and stored and reduces website tracking. With these implementations, the ability for websites to produce targeted, personalized ads is greatly reduced. As a result, Safari has the lowest effective price per thousand impressions (eCPM) compared to other internet browsers. Users are less likely to purchase from advertisements displayed on Safari since they are not as enticing due to the lack of personal information available to formulate targeted ads.

Another feature introduced by Apple in 2014 is App Tracking [3]. This offered users the ability to block and manage the transfer of their information to companies for targeted advertisements [3]. Due to the implementation of this future, some companies have reported a drop in revenue of 30-40% [3].

Google, another big tech player, has also been implementing increased privacy methods to help keep users’ data safe. By 2023, Google plans to implement a privacy initiative called Privacy Sandbox which will limit cookies and replace cross site tracking processes [3]. This is expected to have massive impact on ad revenue for companies since Google Chrome is currently the market leader for browsers with a share of more than 65% [3]. Due to this predominant market usage, many companies are dependent on the browser to collect personalized information and produce targeted ads for maximum revenue generation.

Despite companies beginning to implement strengthened privacy policies, it is still important for users to be knowledgeable regarding privacy issues. Ignorance and misinformation continue to play a detrimental role in a user’s ability to protect him/herself. If users were move aware of the dangers and how to protect themselves, they could be the first line of defense when protecting their personal data. Although it is unlikely that a user can expose sensitive financial information or acquire malware just from having cookies enabled, any user concerned about being tracked or having their information collected can limit the use of cookies or disable them altogether [6]. In an attempt to protect their data and not be tracked, users can also browse in incognito mode, use a virtual private network (vpn), use a private search engine, opt out of targeted advertising, or opt out of data broker sites. [1].

In conclusion, there is a vital cause for concern when it comes to data tracking, user privacy, how our information is stored and used and who has access to said information. Since cookie tracking is not illegal, the more unknowledgeable and complacent users are about accepting cookies and sharing data, the more they lose control over who has access to their information.

**References**

1. C. Stouffer, “Internet tracking: How and why we're followed online,” Norton, 29-Jun-2021. [Online]. Available: https://us.norton.com/blog/privacy/internet-tracking#. [Accessed: Nov-2022].
2. D. Litvinov, “Council post: How internet privacy is changing the online advertising market,” Forbes, 21-Apr-2022. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2021/10/28/how-internet-privacy-is-changing-the-online-advertising-market/?sh=71490ee46755. [Accessed: Nov-2022].
3. Angelia and D. Pishva, "Online advertising and its security and privacy concerns," 2013 15th International Conference on Advanced Communications Technology (ICACT), 2013, pp. 372-377.
4. Tucker, C. E. (2014). Social Networks, Personalized Advertising, and Privacy Controls. Journal of Marketing Research, 51(5), 546–562. <https://doi.org/10.1509/jmr.10.0355>
5. Alexander Bleier, Maik Eisenbeiss, The Importance of Trust for Personalized Online Advertising, Journal of Retailing, Volume 91, Issue 3,2015,Pages 390-409,ISSN 0022-4359,https://doi.org/10.1016/j.jretai.2015.04.001. (<https://www.sciencedirect.com/science/article/pii/S0022435915000263>)
6. “Internet safety: Understanding browser tracking,” GCFGlobal.org. [Online]. Available: https://edu.gcfglobal.org/en/internetsafety/understanding-browser-tracking/1/. [Accessed: Nov-2022].