Who is Following Your Digital Footprints?

Ryan Scott

Grand Canyon University  
ITT-306 Information Security II

Prof. Christine Bakke

# *Abstract*

In the digital age, the protection of personal data has become increasingly important. In this paper, we will examine the extent of data collection on commonly used websites and explore ways to limit unnecessary data sharing. Utilizing tools to reveal the amount of information exchanged on the web, we will take a critical view of companies that make money by providing free products, and the implications this has on personal data. Furthermore, we will identify key behaviors that should be practiced in order to help individuals protect their privacy. The goal of this paper is to raise awareness of the significance of personal data privacy and to empower individuals with the knowledge and tools to take control of their personal data.

**Part 1: Your Digital Footprints**

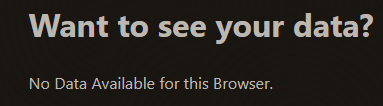
## Digital Footprint Risks

Managing your digital footprint is important to protect your reputation, maintain control over shared personal information, prevent financial loss, and preserve freedom, (Internet Society, 2016). This includes being mindful of your online activity, using privacy settings, being vigilant about online security and privacy, and being aware of how your online activities can be used to track or limit your actions, (Internet Society, 2016).

## 

## Personal Profile Potency, (Oracle | Data Cloud Opt-Out Home, n.d.).

It has become common practice for online advertisers to collect data about users and create personal profiles, including information from social media accounts, browsing histories, location data, and more. Unfortunately (or fortunately, I suppose), when I attempted to view my personal profile, I received the following message:



## 

## 

## 

## Ghostery, (Ghostery, Inc, n.d.).

| **Site Name** | **Category (news, social, shopping, hobby, etc.)** | **Number of Total Trackers Detected** | **Number of Ad Trackers Detected** |
| --- | --- | --- | --- |
| 1. [youtube.com](https://www.youtube.com) | social | 5 | 1 |
| 2. [newgrounds.com](https://www.newgrounds.com) | free game site | 0 | 0 |
| 3. [ign.com](https://www.ign.com/) | news site | 14 | 4 |
| 4. [aseplayer.com](https://www.aseplayer.com) | fan site | 3 | 1 |
| 5. [friendsofanimals.org](https://friendsofanimals.org/) | non-profit | 2 | 1 |

News sites, which rely on ad revenue to support their business model, tend to track and target users more than services that depend on customer purchases. For example, a news site like IGN used a whopping 4 ad trackers, whereas a free game site like Newgrounds, which relies on subscriptions, uses no trackers. This is because news sites rely on ad revenue to generate income, so they need users tracked and targeted with ads to make a profit. On the other hand, game sites that rely on subscriptions do not need to track or target users with ads because they make money from customers purchasing subscriptions.

Additionally, services that generate revenue from advertising are likely to collect more information about their users to better target their ads. This information can include information about their browsing habits, demographic characteristics, and interests. Subscription-based services may not require as much data about their users because they have a steady stream of revenue from customers who have already paid for their services.

## 

## What is Outbrain?

Using machine learning algorithms, Outbrain matches ads and content to users based on their interests, browsing history, and other information, (Outbrain, 2012). As a developer of mobile and browser games, the platform allows InnoGames to reach a highly lucrative audience and increase app downloads, (OutBrain, 2022). By using Outbrain's targeting capabilities, InnoGames can increase the visibility of its apps and games, which will result in more downloads and revenue. Furthermore, Outbrain provides InnoGames with the ability to track and analyze the performance of its advertising campaigns. This can help them to optimize their ad campaigns and make data-driven decisions, (OutBrain, 2022).

***Impressions of Outbrain***

Overall, I would rate OutBrain a solid 3/10. The advertising industry and data collection companies tend to be viewed as neutral actors on the internet, as they provide businesses with the opportunity to reach their target audience and make a profit, (Outbrain, 2012). However, in my opinion, they also diminish a valuable community tool for finding quality: word of mouth. It may be nice to provide users with more relevant content and advertisements, but it is not guaranteed that they will enjoy the item they are shown just because it was suggested by an algorithm. The negative effects of data collection, such as privacy concerns and the potential for companies to misuse data are also not reassuring (to say the least). In my opinion, we might be better off without Outbrain altogether.

**Part 2: The Motives Behind the Ads**

## How Apple and Facebook View Privacy

Some key phrases or taglines that Apple has used to convey its point of view on privacy include:

* *“Privacy. That’s Apple”*
* *“Privacy is a fundamental human right”*
* *“Our apps mind their business. Not yours”*

Some key phrases or taglines that have been used to express Facebook's privacy philosophy include:

* *“Control your information”*
* *"Privacy settings made simple"*
* *“Privacy is a right, not a privilege”*

## Credit Bureaus and Data Collection

## *Who are the Sides?*

Apple is well known for its strong focus on user privacy and security, which it emphasizes throughout its marketing and advertising campaigns. However, Facebook has received criticism in the past for its handling of user information and privacy. As a result, it has taken steps to boost its credibility in this area.

## Source of Income vs Privacy Policy

As a result of relying heavily on advertising as a revenue source, giant tech companies may be more likely to collect and utilize data for targeted marketing. As a result, there may be concerns about how user data is collected, shared, and utilized, and whether users have adequate control over their own information, (Hinze, 2022). A company that makes money by selling user data to a third party is perceived to be less privacy-conscious since it is making money from the personal information of its users, (Hinze, 2022). There are more concerns, but the sad reality is that most users don’t even read the privacy policy of companies before clicking accept. The companies could include a clause that stipulates “they are entitled to appropriate all my ham sandwiches, thereby causing me to be deprived of them” and many would be none the wiser!

## *Comparing Apple vs Facebook’s Revenue Sources*

The revenue sources of Apple and Facebook are quite different, despite their large technology company-like nature.

The two companies are similar in that they both generate a substantial portion of their revenues through the sale of goods and services. A typical Apple example would be iPhones, iPads, Macs, as well as software like the App Store, iCloud, and Apple Music. As far as Facebook is concerned, examples include Instagram, WhatsApp, and… Facebook.

One major difference is that Apple generates a significant portion of its revenue from the sale of hardware and services, whereas Facebook generates the majority of its revenue from advertising, (Hinze, 2022). This means Apple earns the majority of its revenue from the sale of its own products and services, while Facebook generates revenue from the sale of user data.

## The Skeptical View of Ads

Although the advertisements of these companies may appear attractive, they are in fact forms of propaganda. Their marketing teams cannot be trusted, as they have hidden agendas. For instance, these companies may claim to prioritize user privacy, yet they still collect user data for targeted advertising. This illustrates the hypocrisy and lack of transparency which are common in these large tech companies. Furthermore, one should be cautious of the privacy claims made by these companies, as their actions may not always match their words. 0/5.

## Do These Ads Change How I Shop?

I am not particularly concerned with the morality of the companies that advertise their products, but rather, I am most interested in the convenience of the product and its ability to fulfill my needs, whether it be for entertainment or for necessities. I do not believe that the ads have an impact on my decisions when it comes to purchasing and utilizing a product, however, I would be unaware of any invisible force that influences my decisions.

**Part 3: Best Practices for Secure Computing**

## Main Weakness of Company Security Systems

Human error is the main weakness in company security systems, (CBC News, 2019). Social engineering tactics have proven effective in deceiving people into providing sensitive information, such as login credentials or personal information. To exploit human psychology, hackers use tools such as phishing, spear-phishing, and pretexting to convince victims to take actions that benefit them, (CBC News, 2019).

## Technical Solution Implementation Relation

Two-factor Authentication, Anti-Phishing filters, and Security Awareness Training are effective solutions to implement protection against social engineering tactics and human error, (CBC News, 2019). Two-factor Authentication adds an extra layer of security to user accounts by requiring users to provide a second method of authentication, while Anti-Phishing filters are designed to detect and block phishing emails and messages before they reach users' inboxes, (CBC News, 2019). In this case, an ounce of prevention is worth a pound of cure. When prevention fails, Security Awareness Training can educate employees about the dangers of phishing and other malicious activities, as well as how to recognize and avoid them. These solutions enable companies to reduce the risk of security breaches caused by social engineering, as well as ensure that their employees are adequately trained to protect their data, the company's data, and (most importantly) the user’s data, (CBC News, 2019).

## Becoming More Secure

I have implemented several changes in behavior to make my personal information more secure, such as using Nord VPN, relying on Windows Defender, and always checking the URL before entering personal information online, (TheUnlockr, 2019). Unfortunately, at home, my family is using the internet all the time, so it's not ideal to turn the wifi off when it isn’t being used, (BRIGHT SIDE, 2017). However, I try to educate my family about the importance of internet security and remind them to be careful when browsing the internet.

# References

BRIGHT SIDE. (2017, September 7). Always Turn off Wi-Fi When You Don’t Use the Internet. YouTube. <https://www.youtube.com/watch?v=9KKwRoPzSzk>

CBC News. (2019, February 9). How hackers take over your accounts using social engineering (Marketplace). YouTube. <https://www.youtube.com/watch?v=Ck_r2GYLdCI>

Ghostery, Inc. (n.d.). Best Ad Blocker & Privacy Browser. Ghostery. <https://www.ghostery.com/>

Hinze, D. (2022, February 1). What is the Business Model of Facebook, Amazon, Apple, Google and Microsoft? Global Business Group. <https://www.globalbusiness.group/what-is-the-business-model-of-facebook-amazon-apple-google-and-microsoft/>

Internet Society. (2016, January 12). Four Reasons to Care About Your Digital Footprint. YouTube. <https://www.youtube.com/watch?v=Ro_LlRg8rGg>

Oracle | Data Cloud Opt Out Home. (n.d.). <https://datacloudoptout.oracle.com/>

Outbrain. (2012, December 15). What Is Outbrain? YouTube. <https://www.youtube.com/watch?v=kBTYzbT2VsQ>

OutBrain. (2022, October 4). InnoGames Reaches a Highly Profitable Audience and Ensures App downloads. Outbrain. <https://www.outbrain.com/case-studies/innogames/>

TheUnlockr. (2019, May 9). 6 Super Easy Ways to Protect Your Online Privacy. YouTube. <https://www.youtube.com/watch?v=f5OgRumKRGE>