Surveillance Capitalism by Google and Facebook is Ruining The Internet As We Know It

Go to the profile of Christian Stewart ✔️
Christian Stewart ✔️

★

One of the outcomes of computers being involved in the majority of our transactions, is the opportunity for data collection about the transaction and about the parties involved. Unfortunately, the tracking capabilities websites and other internet services use have grown tremendously from that point.

Surveillance capitalism refers to the business of collecting user data through internet connected products and services and then monetizing that information through ad targeting and other means.

> *“As Americans spend more and more of their lives online, it’s vital that we protect the Internet from efforts to turn it into a privacy-free zone where our every keystroke and click is monitored and stored. It’s not just the government that is invading our privacy online, but also companies, which see money to be made in collecting detailed information about*

> *customers in order to build profiles on them." –*[*ACLU,* Consumer Online Privacy]

History of The Surveillance Economy

At some point in the internet's development and evolution, someone decided that there was an opportunity to collect, store and monetize people's data. And there has never been a better way to collect information about people than the internet and the services it provides.

The problem for users is that there is so much value in user data that if people try to hide their identity, websites may prevent people from viewing their content. This model is terrible for users because it completely eliminates the basic right to privacy that everyone should have.

How Did The Internet Become a Two-Way Mirror?

People use the internet to find information, and to answer their questions. However, the internet (the websites we visit) is looking for information about us and about how we use their services. The problem is, there is very little transparency into how websites we visit collect and use our information.

Let's use Facebook for an example. In the past year, there have been multiple occasions when security researchers discovered that Facebook was tracking way more information than they disclosed, or even had consent to track. The company has gotten in trouble and has had to pay fines for violating privacy regulations. Even though people expressed "outrage" and "concern", most people continued using Facebook. The truth is that there are tons of other sites that collect similar amounts of data in similar ways, but these privacy issues just haven't made their way into the news.

Read More:

- ***98 Things Facebook is Tracking About You (And Everyone Else)***
- ***Facebook Isn't The Only Privacy Villain On The Internet***

One result of this "two-way mirror" effect is generalizations about people's behavior and intentions. Companies attempting to market to potential customers, use your data profile to put you into certain buckets of users. If you match a given behavior or tendency, you are grouped together with other users that have the same characteristics. This makes it easier for you to be marketed to, but makes it more difficult for you to find content or information that meets your specific needs.

If the internet is going to be truly user-friendly, grouping people into broad categories or interests is not the right way to get there.

Features of Surveillance Capitalism

Hal R. Varian, Chief Economist at Google, explains these four features of computer mediated transactions. These features completely apply to the system of, and driving forces behind, surveillance capitalism.

1. **The drive toward more and more data extraction and analysis.**
2. **The development of new contractual forms using computer-monitoring and automation.**

3. **The desire to personalize and customize the services offered to users of digital platforms.**
4. **The use of the technological infrastructure to carry out continual experiments on its users and consumers.**

Surveillance Capitalism Drives Innovation

Surveillance capitalism is constantly pushing technology to extract more data and more value from every user. Each business that works with data has to constantly innovate to find more ways to collect information to get ahead of their competitors. Fortunately for internet companies, there are great incentives for discovering new ways to acquire user data, whether that means creating new products, or improving current offerings. Unfortunately for people using the internet, this means that privacy is becoming rarer all the time, and companies are using more and more of their users' data.

Products with massive user bases can benefit greatly from even a small, one percent improvement. More data acquisition means more profits, so companies are constantly looking for wins surrounding their data collection practices.

Customization: Is It Worth It?

The platforms that play a role in surveillance capitalism, are attempting to attract users by saying they are able to customize and tailor their products based on the data they collect from you. This is most noticeable with a tool like Google. It collects information about you through its many tools and services. However one of the explanations the company gives is that it can offer a customized and tailored product to fit your needs and behaviors.

But is a "customized" experience really worth handing over all of your private data? Apparently it is, considering that Google has billions of users and controls nearly 90 percent of the world's search engine market.

Constant Testing & Experimenting

Due to the value of user data, companies and organizations are constantly testing and experimenting with small changes in their products to find out the best and most effective methods to collect data and maximize "conversions" (whatever those may be for a given site). Companies that aren't constantly improving their sites will lose out on potential value collected from user data.

It's not only the privacy demons, like Facebook, that are using constant experiments and changes to maximize the effectiveness of their websites. The infrastructure is simple to implement, so this experimentation is taking place on a broad scale.

This pattern creates a toxic cycle for any company that falls into this trap. As technologies improve for tracking more data, that data paints a more complete picture of each user and thus becomes more valuable. Then, because the data is so valuable, the company wants to collect more data and then continues to innovate its data collection programs. As this progresses, users lose any hint of privacy they may have had and become another "data-profile" in the company's system.

Read More: Who Owns the Future by Jaron Lanier

Who Owns the Future discusses the issues with companies collecting data from the masses, with very little to no resistance. Jaron Lanier points out that by willingly, or just unknowingly, sharing our data with large companies owned by a few wealthy individuals we are putting massive power in the hands of these individuals.

Another issue that Lanier discusses is that the companies like Google, that are collecting people's data aren't properly compensating their users. Google aggregates data from user contributions, and can use that information for monetization and advertising purposes. However, contributors to Google don't get paid, even if they provide tons of value to Google.

If we continue to dump our data into the hands of a few large tech companies, we could contribute to these megacorporations controlling even more of the internet (and the information on the web) than they already do.

Fighting Surveillance Organizations

The best way to combat the government groups, businesses and other organizations from collecting and benefiting from your data is to minimize your internet footprint and focus on privacy. If you have a problem with the tactics that internet companies use to track you and to monetize that information, you can fight back using privacy tools and hiding your identity.

Alternative and Privacy-Friendly Internet Tools

- **Private Messengers:** Private messaging apps, like Signal, make communicating privately simple. They work just like other text messaging or instant messaging platforms, however these private communication tools use encryption to keep your messages confidential.
- **Private Email:** There are plenty of options for private email services. These tools encrypt the contents of your emails and make it nearly impossible for anyone besides you and the email recipient from reading your emails.
- **Encrypted File Storage:** If you use cloud-storage tools like Dropbox or Google Drive, we recommend using alternative tools that use better encryption and file protection. This is especially important if you use mainstream cloud storage tools to store sensitive information. This could include a Google doc with passwords, financial information, or medical records.
- **Private Search Engines:** Private search engines work like any other search engine. Rather than collecting and linking

your IP address, search terms and locations to your identity or data profile, private search engines don't track that information. This means you aren't subjected to ***filter bubbles***, or targeted advertisements from your searches. **Read More:** ***The Best Private Search Engines for 2019***
- **Privacy Browsers:** Browsers like Firefox, Brave, or Chromium offer better privacy than Google Chrome. Because Google allows you to log in to Chrome at the browser level, they can link all of your browsing activity to your Google account.

Using privacy tools does more good than just keeping your identity hidden, it can protect you from other threats online as well. If hackers, or cyber-criminals can't figure out where you're located or who you are, you're less likely to fall victim to an malware, virus, or ransomware attack.

Read More: ***The Best Internet Privacy Tools for 2019***

How To Make Your Browsing Anonymous

Use Ad Blocking Extensions: To fight back against internet advertisers, we recommend using **AdNauseum**. Not only does it block ads, it clicks every ad that would load on the sites you visit. This way, the ad networks receives bogus interaction and click data, rendering the data useless. This costs Google money because it is registering your clicks, but you aren't actually visiting the ad's destination URL. Because this ad goes against Google's business model, it has been banned from Google's Play Store. However, you can still install the extension manually from GitHub.

Inject Some Random Data: There are extensions similar to AdNauseum that instead of confusing ad networks, work to add extra searches to your history in Google to obscure your true browsing. **TrackMeNot** is a browser add-on for Mozilla Firefox that issues randomized search queries to common search engines. This makes search engine tracking much less effective, and as a result, their ads are less specifically targeted. If you can't entirely avoid giving your data to the companies contributing to the "surveillance economy", you can obfuscate that data by adding in random, false data.

Encrypt All of Your Browser Traffic: Browsing websites that don't default to HTTPS can put you at risk for falling victim to a Man-in-The-Middle attack. This is when your browsing isn't using encryption, so anyone with access to your network can view your browsing activity, including information you enter into forms on a website. These attacks are like phishing attacks in that you may start at a site that appears to be secure and then get redirected to another website that doesn't use HTTPS. Use a browser extension like **HTTPS Everywhere** to ensure that all sites you visit are directed to their secure, HTTPS version.

Use a Non-Tracking DNS (Domain Name System): Your ISP's DNS service is just another way for them to collect information about your browsing. Google's DNS is perhaps even more privacy intrusive than your ISP's. Google uses it's Google Fonts API, AMP project and DNS as backdoors to access your private data.

If you're using Linux OS then you can install a local DNS-caching software, like dnsmasq which will reduce the number of DNS look-ups. However, if you're concerned with keeping your browsing as private as possible, caching may not be a smart move.

Randomize Your MAC Address: Whenever you connect to a new network, your IP address changes, but your device’s network address, or MAC address, remains the same. You can add some plausible deniability to your browsing if you randomize and change your MAC address frequently.

Use A VPN: By using a VPN, you can protect your browsing behavior with encryption and hide your local IP address. You should make sure the VPN you choose is reliable and has a privacy-friendly data policy. We put together a list of **the best VPNs for 2019 here**. VPNs have actually been outlawed in some countries with authoritarian governments because it makes it difficult for the government to track down and identify political dissidents or critics.

Compartmentalize Your Data: One of the best ways to fight surveillance organizations is to isolate, or compartmentalize, your sensitive data. For example, for your most sensitive data you should store it on an “air-gapped” machine (a computer that has never connected to the internet). You shouldn’t log in to your Chrome browser, for example, and also log in to your Facebook because then the two companies can link these two data profiles to make their data about you more specific.

Use Two-Factor Authentication

To prevent unwanted access to your online accounts, enable two-factor authentication (2FA) where possible. 2FA works by requiring more than just a password to log in to online accounts. The second factor may be a code texted to your cellphone or email. This is especially important if you believe your passwords may have been compromised.