Amber Kolar

Dr. Goldsmith

February 12, 2019

WR 222

Stop Googling

Using a Google search engine—or Googling—has become a common practice among developed countries worldwide: it is a convenient way to search the web. However, the Google search is one of many confirmed data collection tools which are being used by organizations to track us internet users and create detailed profiles describing us. The massive amounts of user data gathered by big technology companies like Google are constantly being sorted and distributed to both advertisers and government agencies, completely compromising our online privacy. Us internet users do not deserve to be treated this way, so it is a good thing that there are methods we can use which can reduce the data stored about us. One easy way to reclaim some of the privacy we deserve is to switch to a privacy-friendly web browser and search engine, or—in simpler terms—stop Googling.

Google has been found to create detailed profiles which describe their users down to "their most personal habits" (DCN) by having various applications work harmoniously. Digital Content Next (DCN) summarizes a study performed by Douglas Schmidt—a computer science professor form Vanderbilt University—in which Schmidt experimented with Google products to learn the extent of Google's data collection. What he discovered is that Google is collecting data both when Google products are used directly and when they are not. Us users will have our behavior tracked and recorded not only when we make Google searches, but also when we are doing as little as transporting devices connected to Google's Chrome internet browser. So long as the Chrome browser is left running, it is capable of relaying "location information to Google

340 times during a 24-hour period" (DCN). Additionally, when it comes to directly interacting with the web on Chrome, Schmidt found that even while the browser's settings are set to insure privacy, Google still "has the ability to associate anonymous data collected through passive means with the personal information of the user" (DCN). This is possible because Google services—as discovered by Schmidt—can pick up anonymous data from a user's web session and tie it to the user's Google account—should a user ever happen to sign into Google. Google devices also help the company with this data collection process, as they automatically submit device-specific information while online, giving away to Google who anonymous data belongs to (DCN). In short, turning on privacy settings does not make using Google private. Google's many devices and applications make sure of that. The company has created a system that efficiently seeks out user data whenever possible and fits this data together to help Google know and understand us users' behavior (DCN). This alone is disconcerting, as the fact that Google sells our user data to advertisers is public information. However, there is another location—one of greater significance—where Google's data allegedly ends up.

In United States, the National Security Agency (NSA) has been revealed to use a handful of methods to amass data about global internet users and "build what it calls 'a pattern of life', a detailed profile of a target and anyone associated with them" (MacAskill et al.), for numerous individuals. As MacAskill et al. explain in an article, it was 2013 when a man named Edward Snowden left the NSA and leaked classified information about the NSA's data collection practices. Snowden showed the public how the NSA uses what are known as upstream and downstream data collection methods to gather great amounts of information about anyone on the internet (MacAskill et al.). Upstream data collection is carried out by the NSA physically tapping into the fiber-optic cables (which carry internet signals) that run through the United States.

However, the NSA does not stop there: the agency receives a large amount of user data—collected through this same form of mass wiretapping—from the United Kingdom’s Government Communications Headquarters (GCHQ) (MacAskill et al.). The United States and United Kingdom transport much of the world’s internet traffic, so—by working together—the two countries can collect a detailed image of what is sent over the internet. However, this is still not enough to satisfy the NSA. The NSA reaches further by having partner corporations (many of whom were classified even to Snowden when he worked at the NSA) send in information from fiber-optic cable usage as well (MacAskill et al.). The readiness of this agency to work with corporations shows also in how the agency’s downstream data collection occurs. Snowden claims that downstream data collection enables the NSA to have “direct access” (MacAskill et al.) to the data that many large technology companies are already collecting for their own purposes. One of these companies the NSA can allegedly access the data of is Google (MacAskill et al.). What this means is that the overly-detailed profiles Google creates on its users are not only being used for advertising purposes; they are also likely to be adding to the unethically-intricate internet user profiles held by the NSA. All the information the NSA has about us internet users is stored away in case the agency ever decides a user has a suspicious friend of a friend of a friend (This is not an exaggeration! Those who are examined can be this far-removed from targets.), in which case the agency is free to look over the user’s personal information from the internet ranging from habits to emails to phone calls (MacAskill et al.). If we use Google products or services frequently, there may be an increased amount of personal information of ours readily-available for the NSA to view. This is an issue: we deserve to have our privacy respected by all people, no matter how powerful. Opponents to online privacy often say being private is unimportant if a person has nothing to hide. However, what companies and government agencies are being allowed to do constantly stalk us online and—in Google's case—even earn a profit for doing so. If we are stalked offline, it is viewed as unacceptable, even if we have nothing to hide. The standard should be the same on the internet. Many of us internet users have done nothing wrong, yet we are being treated like criminals. Fortunately for us, however, there are solutions to this issue.

Although achieving total privacy online is next to impossible, a great way to limit the information collected about us is to replace Google services with more privacy-friendly alternatives; picking a web browser and search engine other than those owned by Google is a great first step in this direction. A common web browser which can easily be made private is Firefox (Techworld). Firefox is open source, which means that its creator, Mozilla, is completely transparent about what the software does. One thing that the software does not do is constantly send user data to Mozilla. Thanks to Firefox's open details, software developers have also been able to create supplemental addons for Firefox that can be installed to help prevent visited websites from tracking us users (as some websites can perform tracking even without a Chrome browser running them) (Techworld). These addons include HTTPS Everywhere, uBlock Origin, and NoScript (Techworld). A browser that is even more private than Firefox (Techworld) and recommended by Snowden (MacAskill et al.) is Tor. Tor is open source and goes to great lengths to completely hide us users' identities online by not only preventing tracking, but by also masking user IP addresses (Techworld). (IP addresses are like online nametags which websites can normally view for all their visitors.) However, it is worth noting that the Tor browser takes longer to connect to the internet than other browsers because of the extensive process it uses to hide user information (Techworld). Tor is the opposite of Chrome, which not only allows website tracking, but also utilizes it while performing tracking of its own (DCN). Once a replacement for the Chrome browser is set up, it will need a search engine. When it comes to privacy-focused search engines, DuckDuckGo is an excellent option: it is simple and intuitive and saves absolutely no information about us users (Hoffman). However, if we find ourselves unsatisfied with DuckDuckGo's search results, other privacy-friendly search engines such as Startpage can serve as backup (Hoffman). Startpage leverages Google's search engine and therefore provides the same search results as Google, but it serves as a barrier that keeps our user information out of the picture. Startpage also gives us users the option to visit websites anonymously and, like DuckDuckGo, does not save our information (Hoffman). Once we have privacy-friendly browsers and search engines, our online footprints are significantly reduced going forward.

Large quantities of information are constantly being gathered on anyone who uses Google products and services (DCN). This information is sold to advertisers and (according to someone who worked for the NSA) handed off to the United States government (MacAskill et al.). This high level of tracking that us users receive is unacceptable: most of us have done nothing to deserve to be monitored like prison yard criminals. Luckily, we can avoid a portion of this tracking if we use internet browsers like Tor (Techworld) and search engines like DuckDuckGo (Hoffman) in place of the Chrome browser and the Google search engine. If enough people move away from Google, this will also send a message to the company that us users do not appreciate being tracked; one day, perhaps, this could help convince the company to change its ways.

Works Cited

DCN. “Google Data Collection Research.” *Digital Content Next*, 24 Sept. 2018, digitalcontentnext.org/blog/2018/08/21/google-data-collection-research/.

Hoffman, Chris. “5 Alternative Search Engines That Respect Your Privacy.” *How-To Geek*, 5 July 2017, www.howtogeek.com/113513/5-alternative-search-engines-that-respect-your-privacy/.

MacAskill, Ewen, et al. “NSA Files Decoded.” *The Guardian*, Guardian News and Media, 1 Nov. 2013, www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

Techworld. “The Best Secure Browsers 2018.” *Techworld*, 28 Aug. 2018, www.techworld.com/security/best-8-secure-browsers-3246550/.