“Surveillance Capitalism”

Corporations and Digital Privacy

Imagine this. You are on your Instagram feed and you scroll past a couple of ads. Apparently, there’s this huge deal on laptops at Lenovo.com. You scroll further. Another ad about laptops, this time from Best Buy. You have been on the search for a new laptop for a while now, and the other day, you distinctly remember browsing multiple online tech shops using the keyword “laptop”. How did Instagram come to know that?

It is likely that you did not even have to imagine this. Perhaps it has happened so many times before that there was just no need. Targeted advertising has been a common trend in social media, search engines, apps, and websites for a long time now, so long that most people these days will not blink an eye at the fact that it is a tool that corporations use to boost advertising space and product sales. Yet, over the years, targeted advertising has become increasingly precise and invasive, making use of human psychology, internet search histories, and sometimes even smartphone microphones in an attempt to further tailor ads to an individual’s interests. To many users, privacy is a growing concern in software and web services, especially where large corporations driven by an interest to expand profit margins at any cost, are concerned.

Corporations selling and making use of user information on their apps and services has long been a subject of controversy. In the past few years, digital privacy scandals have been picking up steam, coming from the likes of big names such as Facebook and Apple. Indeed, it seems that in the digital age, the biggest concerns regarding digital privacy do not come from rogue hackers or information predators on the dark web, but from companies taking information they already have and utilizing or distributing it in ways that their consumers have not readily consented to. In 2018, Google was said to have purchased millions worth of transaction data from MasterCard, presumably to track purchase habits and further tailor advertisements to their users. In 2014, Facebook reportedly sold the information of some 87 million users to a political consulting company who ostensibly used it as a means for tailoring electoral campaigns. This company was Cambridge Analytica, a name now synonymous with privacy violations and digital vulnerability.

Indeed, the Cambridge Analytica scandal is still shrouded in mystery and layers of complexity. To this day, little is known about what data is collected by corporations, who it is sold to, and what it is later used for. This naturally raises critical questions regarding how secure our information really is in the hands of companies operating services we use on the daily. As more people make use of the web, ‘big data’ (large sets of data that can be used to track consumer behavior on a massive scale) and user information becomes ever more valuable, incentivizing companies to collect information in increasingly unscrupulous ways. Many users suspect that their phones listen in on their conversations, leading to advertisements curtailed to conversations they have had with family and friends. Companies deny this, however, and coincidental ads of things that come up in conversation can sometimes be attributed to other sources, such as search terms and internet history. However, some users are certain that their experiences with their ads were too synchronic with their conversations to be coincidence. When we take into account how carelessly some companies sell user information, would they consider themselves above recording real-life conversations? As devices like Google Home and Amazon Echo grow in popularity, devices that are constantly idle and passively listen for voice commands, the problem with corporations and digital privacy begins to extend to the real world.

It seems that we have entered the age of ‘Surveillance Capitalism’, a term coined by Harvard Business School professor Shoshana Zuboff. In many parts of the world, courts and governments are poorly equipped to deal with digital privacy violations, and lack comprehensive laws regarding user information. It could even be argued that many governments in western liberal democracies actively facilitate such conditions, with legislation specifically built to allow companies as much freedom as possible in an effort to maximize profits and extend global economic influence. Thus, laws against predatory policies as well as legal protection of digital privacy may still be lacking. Several websites, such as Facebook, will not even offer their services to people who do not consent to having their information collected and trafficked.

What can be done about this? It could be proposed that users avoid services suspected of harvesting and trafficking information should they be worried about their digital privacy, but as the internet becomes more and more intertwined with our day to day lives, as companies continue to play coy and operate information trafficking behind closed doors, this is difficult, and will only become more difficult in the future. It seems that large-scale changes to enforcement and legislation are necessary to protect human rights to privacy, demanding that companies be more open with information used and harvested, passing laws restricting and preventing malicious and predatory practices. However, this is a tall order, and while it is still unknown what companies do with information at hand, all we can do is to make our voices known and provide feedback to both our governments and the services we use.

Bibliography

Bergen, Mark. “Google and Mastercard Cut a Secret Ad Deal to Track Retail Sales”. *Bloomberg.* 30, August 2018. https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales

Cyphers, Bennett et al. “Data Privacy Scandals and Public Policy Picking Up Speed: 2018 in Review”. *Electronic Frontier Foundation.* 31, December 2018. https://www.eff.org/deeplinks/2018/12/data-privacy-scandals-and-public-policy-pickinG-speed-2018-year-review

Devries, Will Thomas. “Protecting Privacy in the Digital Age.” *Berkeley Technology Law Journal,* vol. 18, no. 1, 2003. doi:10.15779/Z38T97M

Laidler, John. “High Tech is Watching You”. *The Harvard Gazette*. 4, March 2019. https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/

Meredith, Sam. “Here’s everything you need to know about the Cambridge Analytica scandal”. *CNBC.* 21, March 2018. https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html

Mineo, Liz. “On internet privacy, be very afraid.” *The Harvard Gazette.* 24, August 2017. https://news.harvard.edu/gazette/story/2017/08/when-it-comes-to-internet-privacy-be-very-afraid-analyst-suggests/

Sadowski, Jathan. “Companies are making money from our personal data – but at what cost?” *The Guardian.* 31, August 2016. https://www.theguardian.com/technology/2016/aug/31/personal-data-corporate-use-google-amazon