6-3-2019

Big Tech Surveillance Could Damage Democracy

Chase Johnson
Boise State University, chasejohnson2@boisestate.edu

THE CONVERSATION
Academic rigor, journalistic flair

Companies use data to make a portrait of their users. ImageFlow/shutterstock.com

Big tech surveillance could damage democracy

June 3, 2019 2.10pm EDT

Author

Chase Johnson
Research Associate, Frank Church Institute, Boise State University School of Public Service, Boise State University

Data is often called the oil of the 21st century.

The more tech companies know about their users, the more effectively they can direct them to goods and services that they are likely to buy. The more companies know about their users, the more competitive they are in the market.

Custom-tailored capitalism is what has made Google, Facebook, Amazon and others the richest companies in the world. This profit incentive has turned big tech into a competitive field of mass intelligence gathering. The better and more comprehensive the data, the higher profits will be.

But this business model – what I consider spying machines – has enormous potential to violate civil liberties. Big tech is already being used abroad to enhance the power of repressive regimes, as my work and others' has shown.

While it is not presently a direct threat to U.S. democracy, I worry that the potential for future abuses exists so long as big tech remains largely unregulated.

Big tech's spy machines

Current news is rife with examples of data abuses. In April, NBC News broke a story detailing how Facebook CEO Mark Zuckerberg had used data gathered by the platform to support his friends and defeat his rivals.

This is not Facebook's first privacy PR nightmare. In 2018, data firm Cambridge Analytica used a Facebook app to collect data profiles of over 87 million people, which was later used to distribute targeted political advertising during elections.

Facebook is not alone in the data collection boom. This May, it was revealed that Snapchat employees were using the app's data to obtain location data, pictures and email addresses without users' consent. A new book by former Harvard business professor Shoshana Zuboff goes into great detail of the practices of what she calls "surveillance capitalism." Zuboff writes, "Once we searched Google. Now, Google searches us."

The practice goes beyond someone's taste in music or what they purchase on Amazon. Apps created to help people through mental illness or quit smoking sell data to big tech companies. These users could be potential targets for social stigmatization or targeted advertising that exacerbates heath problems rather than solving them.

In December, The New York Times published an exposé on what one can learn about someone using their collated data from apps and smartphones. By blending location tracking with other online behavior, researchers were able to put together a detailed portrait of the most intimate details of users' lives, such as where their children go to school or who was cheating on their diet. They could even tell which area of a nuclear power plant an individual worked in – information that is typically classified.

Because of these revelations, data that big tech collects poses a national security problem. One open source researcher used data from Strava, a fitness app, to map U.S. military bases around the world as soldiers tracked their runs. Our devices are constantly telling companies where we are and what we are doing. That is not always a good thing.

By blending location tracking with other online behavior, researchers can put together a detailed portrait of the most intimate details of users' lives. Anton Garin/shutterstock.com

For the worst-case scenarios, look abroad

Big tech is a highly unregulated sector of the economy. Existing regulations have struggled to keep up with a rapidly innovating tech sector. In some scenarios, big tech's capabilities are being used by dictators to craft a dystopian digital reality.

Autocratic governments around the world have already begun to use emerging technology to violate human rights. China is a prime example. China integrates AI, biometric data and online activity to track and monitor dissidents and members of ethnic minority communities, who are then sent to reeducation camps.

From my time researching the ways Russia uses these platforms to threaten democracy, I am familiar with the worst-case scenarios of big tech's capabilities. Because platforms' success is predicated on making information go viral, the most successful content can also be some of the most divisive. Russia believes that by disseminating enough false information about the most inflammatory areas of American politics, it can sow chaos in the system. Big tech is the perfect port of entry for such campaigns.

If Russian attacks on social media are combined with AI technology, information attacks could become precision-guided. Nefarious actors could gather the comprehensive profiles that surveillance capitalism has compiled over the years. Fake news would then no longer speak to issues but to individuals, appealing to what makes the user change their mind.

If a monopolistic tech company decided to fully embrace its capacity to spy on its users and leverage that data to a personal or political end, the consequences for democracy could be catastrophic.

Americans got a taste of what an influence attack looks like during the 2016 U.S. presidential election. So long as big tech remains largely unregulated, future influence attacks on American elections will become only more potent.

The business centre Lakhta-2, which reportedly houses news organizations and internet research companies, known for the trolling on social media, in St. Petersburg, Russia. REUTERS/Anton Vaganov

Big tech isn't going anywhere

A surface-level solution to this privacy dilemma would be for people to decouple their online lives from these companies.

For example, DuckDuckGo is an alternative search engine that does not compile user data and promises total privacy. A new browser, Brave, has promised to pay users back for selling data to advertisers.

However, these products are nowhere near as useful for a casual internet user than Google. Simply choosing not to use Google is not that simple.

While there are many different companies in question, they all hold near-monopolistic control over their corner of the market. Amazon dominates online shopping. Facebook dominates interacting with friends and causes. Google dominates web browsing.

Individuals are thus faced with a choice: Radically change their lifestyle and how they interact with the world, or continue to be the target of big tech's spy machines.

Oversight and regulation may seem dramatic and anti-growth at the moment, but I believe that it is a necessary check on big tech – before the worst of its potentials come true.