

Big Tech Uses Data to the Detriment of Consumer Health, But We're Addicted. So What's the Solution?



Opinions expressed by *Entrepreneur* contributors are their own.

As was brilliantly chronicled in the 2020 Netflix documentary *The Social Dilemma*, much of tech today uses data to tap into the human brain in a way that is detrimental to the health of consumers. The examples range from flooding people with ads to creating addictive algorithms on social media to keep them online 24/7. Awareness of these practices, however, is expanding as former tech leaders speak out against it and the demand for data privacy surges.

But what if data privacy isn't the only solution to these

predatory practices?

The status quo

Big tech today uses our data to play upon some of our worst insecurities and dopamine receptors, creating a web-browsing experience that has even been compared to gambling.

The examples of these practices are well-documented: nudging people to subscribe to newsletters, add items to their carts, sign up for services and more. Social-media platforms, such as Twitter and Facebook, have gone from notifying users when someone has interacted with them to notifying users of activity that has nothing to do with them. Big tech's approach of leveraging data and behavioral science to boost its bottom line has come at the expense of consumers, who have quite literally become addicted to their products.

A 2015 study found nearly half of people determined to quit Facebook for just 99 days couldn't even make it through the first few days. And many of those who successfully quit had access to another social-networking site, like Twitter, so they simply displaced their addiction. And, to put it mildly, it's not as though social media has become less addictive since.

Of course, businesses are inherently motivated by profit and won't dial back their exploitation of consumer data out of sheer good will. But they, of all organizations, know the customer is always right. And these days, the customer wants healthier data practices.

Related: 3 Reasons Your Company Should Prioritize Data-Privacy Compliance and Safety Issues

The path forward

So far, governments have addressed this concern by forcing companies to let users decide “what privacy rights to give away, what data you’re willing to part with,” says Colin Gray, a human-computer interaction researcher at Purdue University.

Since 2018, the General Data Protection Regulation (GDPR) has required EU companies to ask people for consent to collect certain types of data. Yet many apps’ banners outside of Europe simply ask users to accept the privacy policies, with no option of opting out. Facebook’s newly-rolled out Privacy Checkup guides users through a series of choices with brightly colored pictures, though the defaults are often set with much less privacy in mind. The endless grid of different checkboxes actually has the effect of overwhelming users.

Even with GDPR’s shortcomings, however, it’s clear the zeitgeist away from data exploitation is starting to be written into the law, and enforced by it. More than three quarters of countries around the world have either drafted or enacted some sort of personal data-privacy protections in recent years, including China, Russia, Brazil and Australia. In September, WhatsApp was fined 225 million euros by the Irish Data Protection Commission for not being transparent enough about its privacy policies. In 2019, Facebook paid a \$5 billion fine for making “deceptive claims about consumers’ ability to control the privacy of their data.”

The path forward is twofold: First, tech companies will have to learn to respect data privacy and ethically collect data. Secondly, when they do inform their products with user data and behavioral science, they should do so in a way that fosters user well-being, rather than exploits it.

Related: 50 Things You Need to Know to Optimize Your Company’s Data Privacy and Cybersecurity

How can healthier data practices become widespread?

Data exploitation has become so ingrained in daily life by now that reversing it seems almost impossible. But there are technologies and approaches already working toward that goal.

Decentralization and privacy have played a major role in conversations surrounding, for example, Web 3.0 – the new internet. Privacy advocates, many of whom come from the cryptocurrency sphere, routinely argue blockchain and decentralization must play a central role in the development of Web 3.0 and the Internet of things (IoT) in order to prevent the kinds of exploitative data practices we see on the current web. Whether through decentralization or something else, this healthy approach that acknowledges data privacy as a cornerstone of Web 3.0 paves a path for freedom from corporate surveillance. Much like the early internet, the new internet emphasizes a community-driven opportunity to initiate change, and that includes the way we handle data.

If the developers building Web 3.0 are for decentralization and privacy, bad behavior could be disincentivized and gradually drowned out. Privacy-focused browsers, such as Brave and DuckDuckGo, are only a sideact to Google today, but there could be a world in which data privacy is the norm on the web.

On the messaging front, cross-platforms like Signal also serve as an alternative to WhatsApp's intrusive missteps, offering end-to-end encryption and privacy. Signal is an open source, peer reviewed and funded entirely by grants and donations. This is the opposite of the monetization model that has commercialized the internet, and it gives people more control over their experiences.

Beyond just privacy, companies that do collect and handle user data must eventually find better uses for that data if they

want to survive – uses that improve people’s lives, rather than turn them into dopamine addicts. That expands beyond just social media and messaging, and into sectors such as medtech.

As healthcare systems begin to screen entire populations for disease, finding ways to act on red flags and prevent further health complications will be key. Behavioral science and data can be leveraged to encourage healthy behavior and checkups. Applications where data is stored privately and only used in the context of the individual’s health journey could initiate conversations and behavioral analyses aimed at improving individual wellbeing, rather than actively harming it.

In the automobile sector, companies like Tesla are using streams of data from its large fleet of vehicles to enact real-time safety improvements. Tesla’s cars vacuum up all sorts of data from their environments with sensors and cameras, which are analyzed by machine-learning algorithms to monitor the car’s condition and detect deviations. It’s able to detect within ten milliseconds the type of crash a driver is about to encounter, the company claims. When the crash occurs, Tesla knows the exact seat position and steering wheel position and deploys the airbags accordingly for optimal safety.

Related: Americans Want Facebook and TikTok Banned Over Privacy Concerns

Tech giants looking to make the most of the data they collect have lessons to learn from companies already using data privately and for healthy applications. The era of big-tech surveillance is nearing its end. Investing more in the well-being of those most attached to a business’s success, rather than short-term profits, will propel true growth going into 2022 and long beyond.

<https://www.entrepreneur.com/article/411979>