

To serve a free society, social media must evolve beyond data mining

April 12 2018, by Aram Sinnreich And Barbara Romzek



Credit: Pixabay from Pexels

As Congress and the public wrestle with the [Facebook-Cambridge Analytica scandal](#), many people are now realizing the risks data collection poses to civic institutions, public discourse and individual

privacy. The U.K.-based political consulting firm didn't just collect personal data from [the 270,000 people](#) who used researcher Aleksandr Kogan's online personality quiz – nor was the damage limited to [87 million of their friends](#). Facebook recently revealed that [nearly all](#) of its [2.2 billion users](#) have had data scraped by "[malicious](#)" people or companies. [The firm itself has joined calls for better privacy regulations.](#)

For years, [watchdogs have been warning](#) about [sharing information](#) with [data-collecting companies](#), firms engaged in the relatively new line of business called some academics have called "[surveillance capitalism](#)." Most casual internet users are only now realizing how easy – and common – it is for unaccountable and unknown organizations to assemble detailed digital profiles of them. They do this by combining the discrete bits of information consumers have given up to e-tailers, health sites, quiz apps and countless other digital services.

As scholars of [public accountability](#) and [digital media systems](#), we know that the business of social media is based on extracting user data and offering it for sale. There's no simple way for them to protect data as many users might expect. Like the social pollution of fake news, bullying and spam that Facebook's platform spreads, the company's [privacy](#) crisis also stems from a power imbalance: Facebook knows nearly everything about its users, who know little to nothing about it.

It's not enough for people to delete their Facebook accounts. Nor is it likely that anyone will successfully [replace it with a nonprofit alternative](#) centering on [privacy, transparency and accountability](#). Furthermore, this problem is not specific [just to Facebook](#). Other companies, including Google and Amazon, also gather and exploit extensive personal data, and are locked in a [digital arms race](#) that we believe threatens to destroy privacy altogether.

Government regulation can help

Governments need to be better guardians of public welfare – including privacy. Many companies using various aspects of technology in new ways have so far [avoided regulation](#) by stoking fears that [rules might stifle innovation](#). Facebook and others have often [claimed that they're better at regulating themselves](#) in an ever-changing environment than a slow-moving legislative process could be.

But these companies have clearly failed to regulate themselves. As Facebook Chief Operating Officer Sheryl Sandberg admitted, "[We did not think enough about the abuse](#)" potential of their data collection practices.

So government regulation is both reasonable and necessary, to reduce the risks that social pollution and data abuse pose to political stability and personal privacy.

Considering new rules

Congress is already discussing how to fight the social pollution of misleading advertising with hidden agendas. The [Honest Ads Act](#) would require both buyers and sellers of online political ads to disclose more information. Facebook's response to the Cambridge Analytica crisis has included [switching from opposing this act to supporting it](#), and even announcing it's [improving transparency](#) before being required to by law.

This is a good start, but it does nothing to protect people's privacy. New rules must govern [privacy policies](#), which today bamboozle consumers into signing away their rights. Most online sites, apps and services have extremely long documents with obscure legal language that most users never read and can't digest. People simply click "agree" and move on.

A new rule could require standard notices, along the lines of [financial](#)

[services disclosures](#), communicating a company's privacy protections in a short and straightforward manner. Another rule could also let users opt out of certain uses or analyses of their data.

Seeking broader protection

Even better than single-issue bills focused on political ads or privacy policies would be sweeping, proactive data protections for online consumers. The European Union's [General Data Protection Regulation](#), which goes into effect on May 25, is a reasonable effort at achieving these ends.

One particularly interesting feature of the GDPR is the "[right to be forgotten](#)," which among other things allows individuals to ask companies to remove information about them from online databases. And the potential penalties for a firm violating the law are significant – [up to 20 million euros](#) or 4 percent of the company's global annual revenue.

However, even a broad law would not address the most fundamental problem. The internet at present is based on a single business model: [surveillance capitalism](#). Online businesses need new ways to make money, without aggregating, exploiting or selling individuals' data.

Changing the business model

To encourage companies to serve democratic principles and focus on improving people's lives, we believe the chief business model of the internet needs to shift to building trust and verifying information. While it won't be an immediate change, social media companies [pride themselves on their adaptability](#) and should be able to take on this challenge.

The alternative, of course, could be far more severe. In the 1980s, when federal regulators decided that AT&T was using its power in the telephone market to hurt competition and consumers, they forced [the massive conglomerate to break up](#). A similar but less dramatic change happened in the early 2000s when cellphone companies were forced to [let people keep their phone numbers](#) even if they switched carriers.

Data, and particularly individuals' [personal data](#), are the precious metals of the internet age. Protecting individual data while expanding access to the internet and its many social benefits is a fundamental challenge for free societies. Creating, using and protecting [data](#) properly will be crucial to preserving and improving human rights and civil liberties in this still young century. To meet this challenge will require both vigilance and vision, from businesses and their customers, as well as governments and their citizens.

This article was originally published on [The Conversation](#). Read the [original article](#).

Provided by The Conversation

Citation: To serve a free society, social media must evolve beyond data mining (2018, April 12) retrieved 27 April 2024 from <https://phys.org/news/2018-04-free-society-social-media-evolve.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--