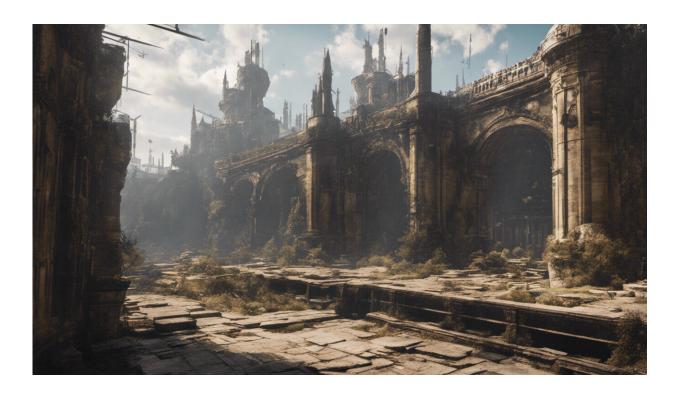# How you helped create the crisis in private data

April 11 2018, by Sarah Igo

Credit: AI-generated image (disclaimer)

As Facebook's [Mark Zuckerberg testifies](#) [before Congress](#), he's likely wondering how his company got to the point where he must submit to public questioning. It's worth pondering how we, the Facebook-using public, got here too.

The scandal in which [Cambridge Analytica harvested data from millions of Facebook users](#) to craft and target advertising for Donald Trump's presidential campaign has [provoked broad outrage](#). More helpfully, it has exposed the powerful yet perilous role of data in U.S. society.

Repugnant as its methods were, Cambridge Analytica did not create this crisis on its own. As I argue in my forthcoming book, "[The Known Citizen: A History of Privacy in Modern America](#)," big corporations (in this case, Facebook) and political interests (in this case, right-wing parties and campaigns) but also ordinary Americans (social media users, and thus likely you and me) all had a hand in it.

The allure of aggregate data

Businesses and governments have led the way. [As long ago as the 1840s](#), credit-lending firms understood the profits to be made from customers' financial reputations. These precursors of Equifax, Experian and TransUnion eventually became enormous [clearinghouses of personal data](#).

For its part, the federal government, from the [earliest census in 1790](#) to the creation of New Deal social welfare programs, has long relied on [aggregate as well as individual data](#) to distribute resources and administer benefits. For example, a person's individual Social Security payments depend in part on [changes in the overall cost of living](#) across the country.

Police forces and national security analysts, too, gathered fingerprints and other data in the name of [social control](#). Today, they employ some of the same methods as commercial data miners to profile criminals or terrorists, [crafting ever-tighter nets of detection](#). State-of-the-art public safety tools include access to social media accounts, online photographs, geolocation information and [cell tower data](#).

Probing the personal

The search for better data in the 20th century often meant delving into individuals' most personal, intimate lives. To that end, marketers, strategists and behavioral researchers conducted [increasingly sophisticated surveys, polls](#) and [focus groups](#). They identified [effective ways](#) to reach specific customers and voters – and often, to [influence their behaviors](#).

In the middle of the last century, for example, motivational researchers sought psychological knowledge about consumers in the hopes of subconsciously influencing them through [subliminal advertising](#). Those probes into consumers' personalities and desires foreshadowed Cambridge Analytica's pitch to commercial and political clients – using data, as its website proudly proclaims, "[to change audience behavior](#)."

Citizens were not just unwitting victims of these schemes. People have regularly, and willingly, revealed details about themselves in the name of security, convenience, health, social connection and self-knowledge. Despite [rising public concerns about privacy and data insecurity](#), large numbers of Americans still find benefits in releasing their data to government and commercial enterprises, whether through [E-ZPasses](#), [Fitbits](#) or [Instagram](#) posts.

Revealing ourselves

It is perhaps particularly appropriate that the Facebook scandal bloomed from a personality test app, "This is your digital life." For decades, [human relations departments and popular magazines](#) have urged Americans to yield private details, and harness the power of aggregate data, to better understand themselves. But in most situations, people weren't consciously trading privacy for that knowledge.

In the linked and data-hungry internet age, however, those volunteered pieces of information take on lives of their own. Individual responses from 270,000 people on this particular test became a gateway to more data, including that belonging to another 87 million of their friends.

Today, data mining corporations, political operatives and others seek data everywhere, hoping to turn that information to their own advantage. As Cambridge Analytica's actions revealed, those groups will use data for startling purposes – such as targeting very specific groups of voters with highly customized messages – even if it means violating the policies and professed intentions of one of the most powerful corporations on the planet.

The benefits of aggregate data help explain why it has been so difficult to enact rigorous privacy laws in the U.S. As government and corporate data-gathering efforts swelled over the last century, citizens largely accepted, without much discussion or protest, that their society would be fueled by the collection of personal information. In this sense, we have all – regular individuals, government agencies and corporations like Facebook – collaborated to create the present crisis around private data.

But as Zuckerberg's summons to Washington suggests, people are beginning to grasp that Facebook's enormous profits exploit the value of their information and come at the price of their privacy. By making the risks of this arrangement clear, Cambridge Analytica may have done some good after all.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: How you helped create the crisis in private data (2018, April 11) retrieved 24 April 2024 from https://phys.org/news/2018-04-crisis-private.html