How 2021 was the year governments really started to wise up against big tech

David Tuffley, *Griffith University*

After all the bad press tech companies have received, would anyone still be surprised to learn the outwardly smiling face of social media conceals a sophisticated data-collection industry?

This year's headlines delivered news of an array of concerning data and privacy violations from the world's biggest tech players. But interestingly, it also seemed to be the year governments around the world addressed the problem head on.

Google in trouble with the ACCC

In April, Australia's consumer watchdog, the Australian Competition and Consumer Commission, took Google to Federal court, citing Australian Consumer Law relating to consumer privacy.

It was alleged Google did not clearly identify how it collected and used users' location data collected through Android devices in 2017 and 2018. Google was accused of leading users to mistakenly believe their personal location data was not being collected, when it actually is.

The Court found Google's conduct was liable to misleading the public. Here's how.

A tale of two settings

There are two settings on Android devices that govern how data is collected: location history and web and app activity.

Stepping through the setup screens, the user is shown their location history as being switched off by default. But it's not made clear the web and app activity setting (located elsewhere) is *on* by default, and could also be used to collect location data – even if location history is switched off.

So the user might believe location tracking is switched off, but in reality tracking may still be performed because of the default web and app activity setting (which they might not know about).

Android 12 (released in October) now has a new privacy dashboard that goes some way towards remedying the permissions transparency issue. It shows the user which apps have accessed location services, and allows them to deny further access.

However, the web and app activity setting is still located elsewhere and not easily found. It is still switched on, by default, and able to track users' movements.

To switch this setting off, follow the instructions here. But be aware that once you do this Google Maps might not work as well for you, and ads will become less relevant, along with search recommendations.

In separate proceedings in July, Google was once again sued by the ACCC for allegedly not disclosing it receives sensitive information about users from third-party websites and apps. Google was accused of using this information commercially without making the process clear to users.

The company was also hit with yet another major antitrust lawsuit, in which its influence over app developers was called into question.

Specifically, the multi-state lawsuit accused Google of abusing its market power to stifle competition and force users and developers to engage with Google's own high-fee payment processing system.

This was one in a number of US state and federal antitrust cases against the company, with the first one brought forward in October last year.

'Astronomical profits before people'

Meanwhile, Meta Platforms (or Facebook) is still reeling from Francis Haugen's damning testimony to the US Congress in October.

A former manager at Facebook, Haugen accused Facebook of a catalogue of antisocial behaviour, in which it knowingly allowed the amplification of hate speech, propagation of misinformation and instigation of political unrest on the platform.

Haugen claimed employees had expressed concerns internally, but these were disregarded, or at least were not enough to change the situation. She is due to give a follow-up testimony in December.

Meta CEO Mark Zuckerberg refuted the allegations, saying they are "just not true". He wrote in a blog post:

> The argument that we deliberately push content that makes people angry for profit is deeply illogical. We make money from ads, and advertisers consistently tell us they don't want their ads next to harmful or angry content.

More recently, the Washington Post reported on another anonymous whistleblower and former Facebook employee, who came out with a sworn affidavit saying Facebook puts profits ahead of stopping hate speech, misinformation and other threats to the public interest.

TikTok and children's data

In April, the former children's commissioner for England, Anne Longfield, launched a legal action concerning the way video-sharing app TikTok collects and uses the data of children using the app.

The lawsuit alleges TikTok (which is now said to have more than one billion users) collects sensitive personal information including children's phone numbers, where they live, and unspecified "biometric data" without sufficient transparency, and without asking consent as required by UK law.

TikTok's policies simply state it will collect information "you share with us from third-party social network providers, and technical and behavioural information about your use of the platform". But this does not sufficiently explain the nature and extent of the data collection.

The lawsuit also claims there's no transparency regarding how users' personal information is used. Longfield described TikTok as "a data collection service that is thinly veiled as a social network".

TikTok responded by saying user privacy and safety were its top priorities, and it has "robust policies, processes and technologies in place to help protect all users".

There's also the larger debate on whether TikTok – owned by Beijing-based company ByteDance – may be using user data for censorship, spreading propaganda among users, or to spy on users by feeding data back to the Chinese government (which is a ByteDance shareholder).

The essence of the problem

Currently, the fact people *could* read a terms and conditions document before clicking “agree” apparently amounts to informed consent, in the legal sense. The result is most users consent to their data being collected and used in numerous ways, but are none the wiser of the specifics.

Regulators must oblige platforms to be upfront and transparent about how user data is collected, used, and whom it is forwarded to (and for what purpose).

This could be achieved quite easily by including this information in plain language on the very same terms and conditions page. But as it stands it’s too easy for platforms to hide behind loose definitions of informed consent.

Although if the events of the past year are anything to go by, this may be starting to change.

David Tuffley, Senior Lecturer in Applied Ethics & CyberSecurity, *Griffith University*