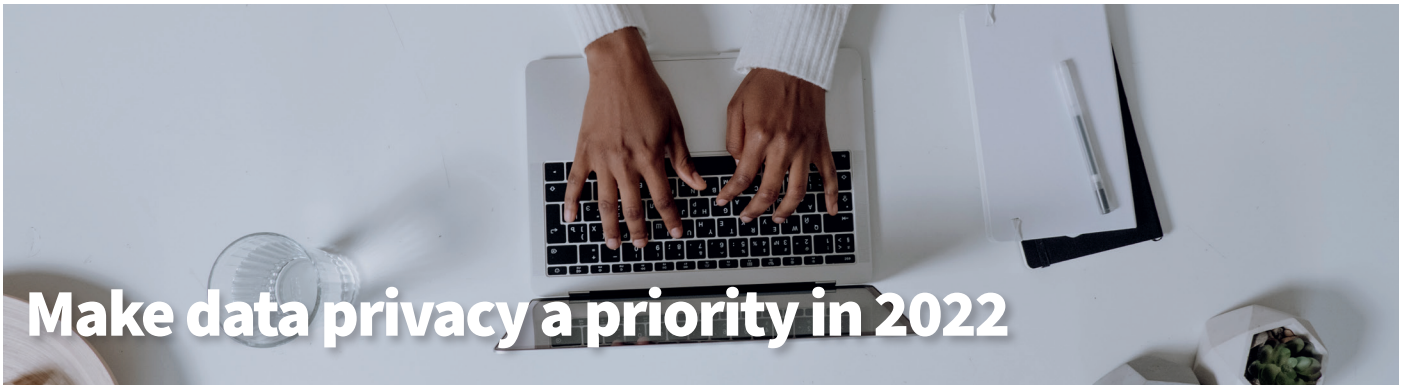
RAYMOND JAMES



Make data privacy a priority in 2022

As our lives become more digitally integrated, our data becomes more valuable.

Often, data collectors say that the vast amount of information they take in is tightly secured or anonymised before it is packaged and resold. However, researchers from the Massachusetts Institute of Technology discovered in 2018 that individuals could be identified by combining two anonymised data sets covering the same population. A 2019 series from The New York Times went further, exposing the risk to privacy on a massive scale if a major tech firm's anonymised location data was stolen and cross-referenced to publicly available property records.

As long as consumer concerns about privacy remain limited, there is little incentive for companies to cull their data collecting habits. The market for privacy-conscious products is growing as demand increases, expect that to continue.

In the meantime, here are some best practices to help minimise the amount of your information that data collectors can access.

TURN OFF PERSONALISED ADS

Many of the largest ad space sellers, particularly those providing tech services like email and social media, now give the option to depersonalise your advertising experience. They'll still collect the information, but there are some limits to how specifically targeted the ads can be. This is becoming a battleground topic in the tech industry, as companies that don't rely on ad sales are finding privacy to be a strong selling point.

SKIP THE QUIZ

That silly online quiz to help you determine which fast food mascot you are may be mining serious information about you. Though it's a bad practice, many online accounts rely on security questions to establish your identity, questions that are easily snuck into online quizzes.

> The market for privacy-conscious products is growing as demand increases, expect that to continue.

GO DIGITAL AND SHRED THE REST

Your home or driveway may be advertising your wealth, making your mailbox and your trash a target. Despite the well-publicised thefts of user data in recent years, an online account is in many ways more secure than an unlocked mailbox, and generally less personal. Privacy experts recommend making the switch, and when you do get mail that contains information about your health, finances or family, make sure to shred it before you toss it.

KNOW WHAT HEALTH DATA IS BEING COLLECTED

You can now choose if data from your health records is used by the NHS and others for research and planning. There is no similar regulation for health data you share with your fitness device manufacturer. It's worth your while to make sure you understand what information is being collected and for what purposes. Go into the device settings to see what options you have. The EULA, or end-user license agreement, will have more information if you can read legalese.

Sources: The New York Times; Vox; The Washington Post; Fast Company; Massachusetts Institute of Technology; Consumer Reports; NPR; Goldman Sachs; ZDNet.com; NHS.uk