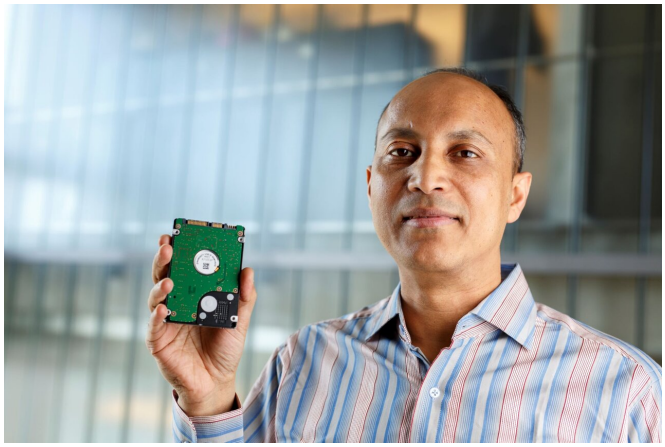
Government websites and apps use the same tracking software as commercial ones, according to new research

17 May 2022, by Patrick Lejtenyi



Mohammad Mannan, associate professor at the Concordia Institute for Information Systems Engineering (CIISE) at the Gina Cody School for Engineering and Computer Science. Credit: Concordia University

It's no secret that the commercial websites and mobile apps we use every day are tracking us. Big companies like Facebook and Google depend on it. However, as a new paper by a team of Concordia researchers shows, businesses are not the only ones gathering up our private data. Governments across the world are incorporating the same tracking tools and empowering large businesses to track users of government services, even in jurisdictions where lawmakers are enacting legislation to restrict commercial trackers.

The paper's authors performed privacy and security analyses of more than 150,000 government websites from 206 countries and more than 1,150 Android apps from 71 countries. They found that 17 percent of government websites and 37 percent of government Android apps host Google trackers. They also noted more than a quarter—27 percent—of Android apps leak sensitive information to third parties or potential network attackers. And they identified 304 sites and 40 apps flagged malicious by VirusTotal, an internet security website.

"The findings were surprising," says the paper's co-author Mohammad Mannan, associate professor at the Concordia Institute for Information Systems Engineering (CIISE) at the Gina Cody School for Engineering and Computer Science. "Government sites are supported by public money, so they do not need to sell information to third parties. And some countries, especially in the European Union, are trying to limit commercial tracking. So why are they allowing it on their own sites?"

Unintentional but invasive

The researchers began their analysis by building off a seed list containing tens of thousands of government websites using automated searching and crawling and other methods between July and October 2020. They then performed deep crawls to scrape links in the HTML page source. The team used instrumented tracking metrics from OpenWPM, an automated, open-source software used for web-privacy measurements, to collect information such as scripts and cookies used in the websites' code as well as device fingerprinting techniques.

They tracked Android apps by looking for Google Play store URLs found in government sites and then examining the developers' URLs and email addresses. When possible, they downloaded the apps—many were geo-blocked—and analyzed them for embedded tracking software-development kits (SDKs).

The analyses revealed that 30 percent of government websites had one or more JavaScript

trackers on their landing pages. The most known trackers were all owned by Alphabet: YouTube (13 percent of websites), doubleclick.net (13 percent) and Google (close to four percent). They found some 1,647 tracking SDKs in 1,166 government Android apps. More than a third—37.1 percent—were from Google, with others from Facebook (6.4 percent), Microsoft (2.1 percent) and OneSignal (2.9 percent).

Mannan notes that the use of trackers may not always be intentional. Government developers are most likely using existing suites of software to build their sites and apps that contain tracking scripts or include links to tracker-infused social media sites like Facebook or Twitter.

No other options

While the use of trackers is widespread, Mannan is particularly critical of jurisdictions like the EU and California that profess to have strong privacy laws but in practice are not always significantly different from others. And since users can use only government portals for important personal obligations such as paying taxes or requesting medical care, they are at added risk.

"Governments are becoming more aware of online threats to privacy, but at the same time, they are enabling these potential violations through their own services," he says.

Mannan urges governments to frequently and thoroughly analyze their own sites and apps to guarantee privacy safety and to ensure that they are complying with their own laws.

The research was published in the *Proceedings of the ACM Web Conference 2022*.

More information: Nayanamana Samarasinghe et al, Et tu, Brute? Privacy Analysis of Government Websites and Mobile Apps, *Proceedings of the ACM Web Conference 2022* (2022). DOI: 10.1145/3485447.3512223

Provided by Concordia University