Fingerprinting to track users online is on the rise. Here’s what to do

The technique, which involves looking at device characteristics and triangulating data to follow users, happens invisibly in the background in apps and on websites.

Fingerprinting can create user profiles. • NYT/ELLEN HARVEY

If there’s one lesson to learn about digital privacy, it’s that we can never grow complacent. Even if we secure our data so we are not tracked online, the ad tech industry will find ways to monitor our digital activities. And so it is with the rise of so-called fingerprinting, a tracking method about seven years old, but it was rarely discussed until recently. Online, the ad tech industry track users with what security researchers call a next-generation fingerprinting, or “fingerprinting.”

Growing slowly

Fingerprinting involves looking at the many characteristics of a mobile device or computer, like the screen resolution, operating systems, and location. This information is used to create a profile that helps identify users even after they have deleted their data. But fingerprinting doesn’t stop there.

Blocking solutions

There are restrictions to fingerprinting so that you can prevent content for apps and websites work properly.

Fingerprinting can be done directly inside apps, but that’s up from about 1.6% in 2016 to 2.8% last year, according to Mozilla. And an unknown number of mobile apps also use fingerprinting.

Growing slowly

Security researchers discovered fingerprinting as a tracking method about seven years ago, but it was rarely discussed until recently. On mobile apps are only beginning to emerge. ‘Disconnect’ offers mobile apps for blocking fingerprinting so that you can prevent content for apps and websites work properly.

Fingerprinting to track users online is on the rise. Here’s what to do

The technique, which involves looking at device characteristics and triangulating data to follow users, happens invisibly in the background in apps and on websites.

Fingerprinting can create user profiles. • NYT/ELLEN HARVEY

If there’s one lesson to learn about digital privacy, it’s that we can never grow complacent. Even if we secure our data so we are not tracked online, the ad tech industry will find ways to monitor our digital activities. And so it is with the rise of so-called fingerprinting, which security researchers are calling a next-generation tracking technology.

Fingerprinting involves looking at the many characteristics of a mobile device or computer, like the screen resolution, operating system, and model, and triangulating this information to pinpoint and follow users as they browse the web and use apps.

Fingerprinting involves looking at device characteristics and triangulating data to follow users, happens invisibly in the background in apps and on websites.

Growing slowly

Security researchers discovered fingerprinting as a tracking method about seven years ago, but it was rarely discussed until recently. On mobile apps are only beginning to emerge. ‘Disconnect’ offers mobile apps for blocking fingerprinting so that you can prevent content for apps and websites work properly.

Fingerprinting to track users online is on the rise. Here’s what to do

The technique, which involves looking at device characteristics and triangulating data to follow users, happens invisibly in the background in apps and on websites.

Fingerprinting can create user profiles. • NYT/ELLEN HARVEY

If there’s one lesson to learn about digital privacy, it’s that we can never grow complacent. Even if we secure our data so we are not tracked online, the ad tech industry will find ways to monitor our digital activities. And so it is with the rise of so-called fingerprinting, which security researchers are calling a next-generation tracking technology.

Fingerprinting involves looking at the many characteristics of a mobile device or computer, like the screen resolution, operating system, and model, and triangulating this information to pinpoint and follow users as they browse the web and use apps.

Fingerprinting involves looking at device characteristics and triangulating data to follow users, happens invisibly in the background in apps and on websites.

Growing slowly

Security researchers discovered fingerprinting as a tracking method about seven years ago, but it was rarely discussed until recently. On mobile apps are only beginning to emerge. ‘Disconnect’ offers mobile apps for blocking fingerprinting so that you can prevent content for apps and websites work properly.

Fingerprinting to track users online is on the rise. Here’s what to do

The technique, which involves looking at device characteristics and triangulating data to follow users, happens invisibly in the background in apps and on websites.

Fingerprinting can create user profiles. • NYT/ELLEN HARVEY

If there’s one lesson to learn about digital privacy, it’s that we can never grow complacent. Even if we secure our data so we are not tracked online, the ad tech industry will find ways to monitor our digital activities. And so it is with the rise of so-called fingerprinting, which security researchers are calling a next-generation tracking technology.

Fingerprinting involves looking at the many characteristics of a mobile device or computer, like the screen resolution, operating system, and model, and triangulating this information to pinpoint and follow users as they browse the web and use apps.

Fingerprinting involves looking at device characteristics and triangulating data to follow users, happens invisibly in the background in apps and on websites.

Growing slowly

Security researchers discovered fingerprinting as a tracking method about seven years ago, but it was rarely discussed until recently. On mobile apps are only beginning to emerge. ‘Disconnect’ offers mobile apps for blocking fingerprinting so that you can prevent content for apps and websites work properly.

Fingerprinting to track users online is on the rise. Here’s what to do

The technique, which involves looking at device characteristics and triangulating data to follow users, happens invisibly in the background in apps and on websites.

Fingerprinting can create user profiles. • NYT/ELLEN HARVEY

If there’s one lesson to learn about digital privacy, it’s that we can never grow complacent. Even if we secure our data so we are not tracked online, the ad tech industry will find ways to monitor our digital activities. And so it is with the rise of so-called fingerprinting, which security researchers are calling a next-generation tracking technology.

Fingerprinting involves looking at the many characteristics of a mobile device or computer, like the screen resolution, operating system, and model, and triangulating this information to pinpoint and follow users as they browse the web and use apps.

Fingerprinting involves looking at device characteristics and triangulating data to follow users, happens invisibly in the background in apps and on websites.

Growing slowly

Security researchers discovered fingerprinting as a tracking method about seven years ago, but it was rarely discussed until recently. On mobile apps are only beginning to emerge. ‘Disconnect’ offers mobile apps for blocking fingerprinting so that you can prevent content for apps and websites work properly.

Fingerprinting to track users online is on the rise. Here’s what to do

The technique, which involves looking at device characteristics and triangulating data to follow users, happens invisibly in the background in apps and on websites.

Fingerprinting can create user profiles. • NYT/ELLEN HARVEY

If there’s one lesson to learn about digital privacy, it’s that we can never grow complacent. Even if we secure our data so we are not tracked online, the ad tech industry will find ways to monitor our digital activities. And so it is with the rise of so-called fingerprinting, which security researchers are calling a next-generation tracking technology.

Fingerprinting involves looking at the many characteristics of a mobile device or computer, like the screen resolution, operating system, and model, and triangulating this information to pinpoint and follow users as they browse the web and use apps.

Fingerprinting involves looking at device characteristics and triangulating data to follow users, happens invisibly in the background in apps and on websites.

Growing slowly

Security researchers discovered fingerprinting as a tracking method about seven years ago, but it was rarely discussed until recently. On mobile apps are only beginning to emerge. ‘Disconnect’ offers mobile apps for blocking fingerprinting so that you can prevent content for apps and websites work properly.

Fingerprinting to track users online is on the rise. Here’s what to do

The technique, which involves looking at device characteristics and triangulating data to follow users, happens invisibly in the background in apps and on websites.

Fingerprinting can create user profiles. • NYT/ELLEN HARVEY

If there’s one lesson to learn about digital privacy, it’s that we can never grow complacent. Even if we secure our data so we are not tracked online, the ad tech industry will find ways to monitor our digital activities. And so it is with the rise of so-called fingerprinting, which security researchers are calling a next-generation tracking technology.

Fingerprinting involves looking at the many characteristics of a mobile device or computer, like the screen resolution, operating system, and model, and triangulating this information to pinpoint and follow users as they browse the web and use apps.