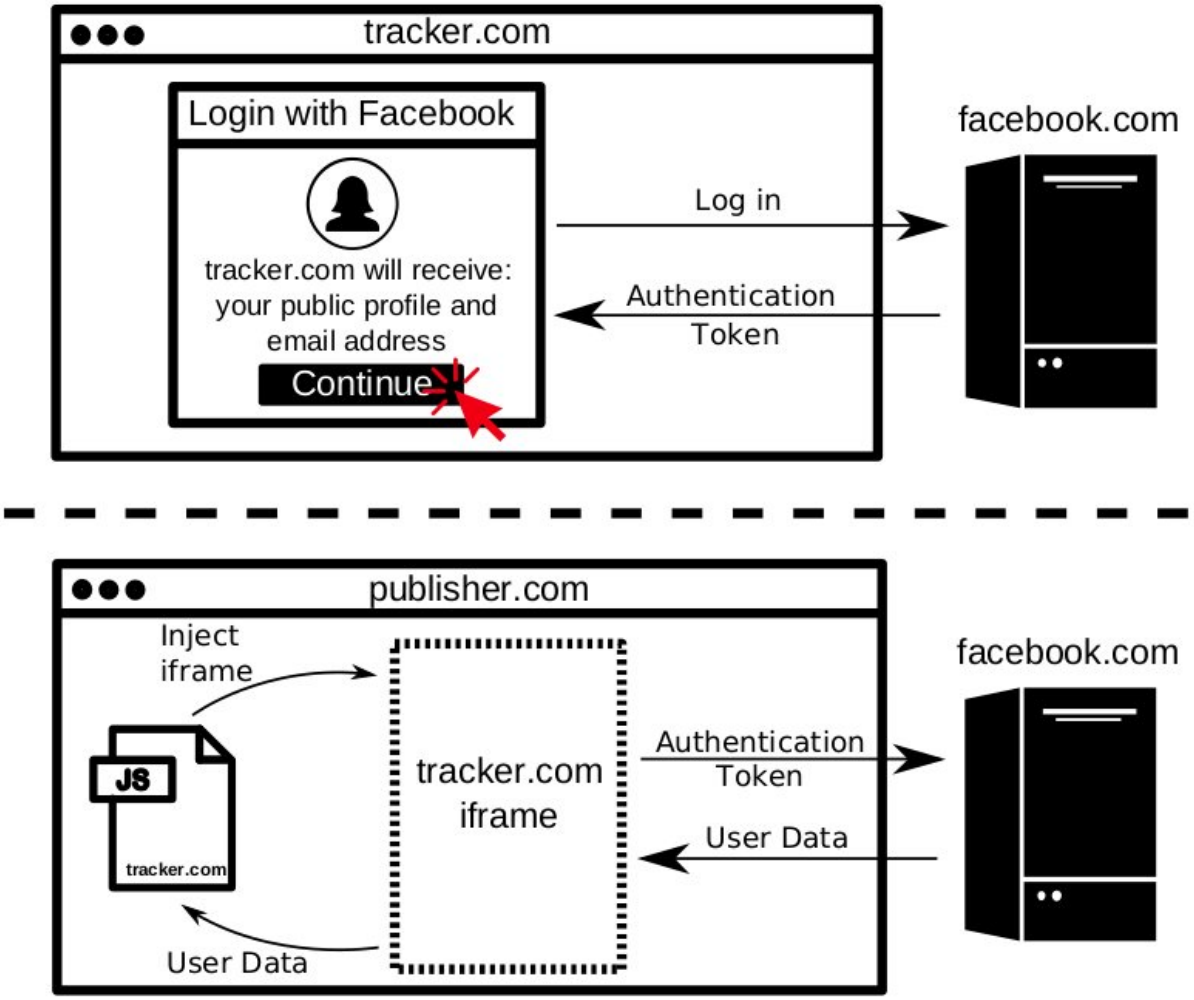
Princeton's tech watchers shine glaring light on web tracking, data slurping

April 21 2018, by Nancy Owano



Top panel: Bandsintown's website (represented as tracker.com) allows visitors to learn about local concerts and follow artists they might be interested in. To follow an artist, users are required to Login with Facebook and give the

Bandsintown Facebook app access to their profile, city, likes, email address, and music activity. At this point Bandsintown has access to the necessary authentication tokens to access Facebook account information. Bottom panel: Bandsintown offers an advertising service called “Amplified”, which is present on many of the top music-related sites including lyrics.com, songlyrics.com and lyricsmania.com. When a Bandsintown user browses to a website that embeds Bandsintown’s Amplified advertising product, the advertising script embeds an invisible iframe which connects to Bandsintown’s Facebook application using the authentication tokens established earlier, and grabs the user’s Facebook ID. The iframe then passes the user ID back to the embedding script. Credit: Freedom to Tinker

Hidden online trackers are hardly secure in their hiding place, not after this week's headlines for stories about how Facebook user information can be nabbed. The information can be obtained on various websites that support logging-in through the social platform.

Many websites offer "login with Facebook" but Princeton University researchers find something to worry about here. *Business Insider*, one of the numerous sites taking a look at the Princeton researchers' findings, explained how "trackers can harvest user data like profile picture, name, email address, age, and gender – probably much more than people intend to give away when they log in to sites using Facebook."

Stepping back to square one, it was the security researchers at Freedom to Tinker whose findings grabbed the attention of tech watchers.

Freedom to Tinker is hosted by Princeton's Center for Information Technology Policy; it gazes on digital technologies in public life. Third-party trackers abuse the Facebook login, they reported on Wednesday. There is no way to sugar-coat it; the post called it "surreptitious data collection by third-party scripts."

The result is the exfiltration of personal identifiers from websites through "login with Facebook" and other such social login APIs.

According to *Freedom to Tinker*, they can't say how the trackers use the information they collect, but they could examine their marketing material to understand how it may be used—for example, collecting data to help publishers better monetize their users.

The researchers discussed types of events. The researchers identified seven third parties that were accessing Facebook user data, and they found one third party that uses its own Facebook "application" to track users around the web.

Freedom to Tinker's post stated that "This unintended exposure of Facebook data to third parties is not due to a bug in Facebook's Login feature. Rather, it is due to the lack of security boundaries between the first-party and third-party scripts in today's web."

Writing in *TechCrunch*, Josh Constine thought that "Facebook could have identified these trackers and prevented these exploits with sufficient API auditing."

Make no mistake, though, the issue of tracking users without their direct consent or even knowledge is an issue that does not rest only at Facebook, as several observers pointed out in their comments over Princeton team findings. Also, the researchers had limited investigations to Facebook Login because it was the most widely used social SDK on the web—not because it is the only one that involves this wider issue of tracking.

As stated in *Freedom to Tinker*, "In this post we focus on websites which use Facebook Login, but the vulnerabilities we describe are likely to exist for most social login providers and on mobile devices."

TechCrunch: There are other tech giants relying on user data and they operate developer platforms that can be tough to police.

"Zuckerberg makes an easy target because the Facebook founder is still the CEO, allowing critics and regulators to blame him for the social network's failings. But any company playing fast and loose with user data should be sweating."

Princeton did have some recommendations to make for future ways to deal with questions of privacy. "Still, there are steps Facebook and other social login providers can take to prevent abuse: API use can be audited to review how, where, and which parties are accessing social login data. Facebook could also disallow the lookup of profile picture and global Facebook IDs by app-scoped user IDs. It might also be the right time to make Anonymous Login with Facebook available following its announcement four years ago."

What does Facebook say about reports that users are tracked? Constine reported that "Facebook confirms to *TechCrunch* that it's investigating a security research report that shows Facebook user data can be grabbed by third-party JavaScript trackers embedded on websites using Login With Facebook."

Constine went on to say that a "Facebook spokesperson now tells us 'Scraping Facebook user data is in direct violation of our policies. While we are investigating this issue, we have taken immediate action by suspending the ability to link unique user IDs for specific applications to individual Facebook profile pages, and are working to institute additional authentication and rate limiting for Facebook Login profile picture requests.'"

More information: No boundaries for Facebook data: third-party trackers abuse Facebook Login, freedom-to-tinker.com/2018/04/ …

buse-facebook-login/