Source: *The Straits Times,* pA16
Date: 19 October 2021

Taking that Squid Game quiz? Ad Tech is watching you

Digital consumers are being targeted by surveillance advertising. There are dangers in this. What protection is available here and overseas?

Chew Han Ei
For The Straits Times

Not many consumers know about the global ecosystem of data firms that are trading their data from various websites and apps. It is impossible for individuals to know who has their data, how their data is being transferred or who is analysing their data. ST PHOTO: KELVIN CHNG

When we complete a seemingly innocuous Squid Game quiz to find out which character in the popular TV show we are closest to, we are also giving up more data that can be used to profile us.

When our friends also do the quiz and we interact with their results, we are giving up data about our relationships with like-minded people who enjoy the same content and are likely to be influenced by similar ads.

This targeting is what is known as surveillance advertising.

This is the practice of extensively tracking and profiling individuals and groups, and "microtargeting" ads at them based on their behavioural history, relationships and identity, according to Accountable Tech, a non-government organisation.

Global concern about the dangers of surveillance advertising is growing.

The most compelling argument against surveillance advertising is that it enables the marketing of harmful products and services to children and young people. Back in 2017, Facebook reportedly told advertisers that it could monitor posts to determine when young people are feeling "insecure" and "worthless". In the Facebook Files recently released by the Wall Street Journal, researchers inside Instagram found the app to be harmful to the mental health of teenagers, especially girls.

Here in Singapore, surveillance advertising is not explicitly prohibited under existing laws.

HOW IS IT USED?

Surveillance advertising is built on the immense volumes of data that Big Tech companies collect about their users ranging from geolocation to inferred interests based on matching online and offline data sets.

Being able to track user activity across platforms and services allows tech companies to create very detailed user profiles. Ads can then be hyper-personalised and microtargeted at specific users at specific times.

In traditional advertising, ads are placed in a predetermined medium and for a fixed period of time, for example by buying ad space in a home and decor magazine in order to reach homeowners.

Surveillance advertising is different in that the ads follow the consumers. In fact, using profiled information, Ad Tech companies can tailor ads and attempt to target consumers when they are deemed to be most susceptible to behaving or reacting to the messaging in certain ways.

COUNTERING THE DANGERS

The European Union is proposing a Digital Services Act to protect the fundamental rights of users and create a safer digital space.

In the United States, there is a new coalition of organisations pushing for a ban on surveillance advertising on the grounds that selling hyper-personalised ads is an unfair method of competition.

Advocates for banning surveillance advertising also argue that the practice infringes privacy and data protection, funds misinformation, and promotes harm to children, among others.

In Singapore, experts have highlighted the risks of data misuse that can lead to a loss of trust in digital technologies. Case in point, a study by Okta, a company that provides user authentication login solutions, showed that Asian consumers are most likely to lose trust in brands that intentionally misuse or sell their personal data. Following a data breach, consumers may also permanently stop using the digital services and delete the apps.

The call to protect children and adolescents from global harmful advertising has also been sounded by a United Nations report, A Future For The World's Children?. It points to how advertisers bombard children and adolescents with ads on social media to promote harmful products, from fast food to tobacco and alcohol. Data on children obtained from electronic games is also being sold to global tech giants.

The report's lead author, Professor Anthony Costello, argues that "children have the right not to be bombarded every day on their phones with advertisements or to have their data stolen".

Another critical problem of surveillance advertising is that data flows are invisible to the consumers. Already, not many consumers know about the global ecosystem of data firms that are trading their data from various websites and apps. It is impossible for individuals to know who has their data, how their data is being transferred or who is analysing their data. They would also not know when they have been targeted with hyper-personalised ads or why they were shown an ad.

The most compelling argument against surveillance advertising is that it enables the marketing of harmful products and services to children and young people.

The ad placement processes are fully automated. Data is fed into systems in which algorithms decide where an ad is placed.

Advertisers and the owners of the websites often do not know where the ads are being placed – only the Ad Tech companies know. This lack of control can lead to brand damage if the ads are displayed next to disinformation or other problematic content.

PROTECTING SINGAPORE CONSUMERS

The advertising industry in Singapore is self-regulated and the Advertising Standards Authority of Singapore (ASAS) advises the Consumer Association of Singapore on matters related to marketing on social media.

While the Guidelines on Interactive Marketing Communication and Social Media issued by the ASAS in August 2016 list provisions for the protection of children's personal information, they are silent on surveillance advertising.

The topic of behavioural targeting is mentioned in the advisory guidelines on the Personal Data Protection Act for selected topics, which state that where behavioural targeting involves the collection and use of personal data, the individual's consent is required.

It is not known if either of these guidelines are enforced on the surveillance advertising that is occurring in Singapore.

INCREASING TRANSPARENCY, ACCOUNTABILITY

New legislation to curb surveillance advertising that has been proposed by other countries ranges from imposing greater transparency requirements to an outright ban.

The EU's draft Digital Services Act in its current form will impose requirements to disclose information about ads, such as the identity of the advertiser and the criteria used to determine the display of the ad, including if it is based on profiling.

In the US, the Ban Surveillance Advertising Coalition is advocating a rule to "prohibit businesses from sharing user data, for the purposes of advertising, to any business line, website, advertising technology, or tracker other than the business or service with which a user intentionally interacts".

It is uncertain how legislation will evolve but locally, the relevant government agencies such as the Ministry of Trade and Industry and the Personal Data Protection Commission should study the digital advertising ecosystem to understand the implications for Singapore consumers. The French data protection authority CNIL is studying this in its research lab. And while policymakers go through the due processes, advertisers and website or app owners can already adopt some best practices.

One alternative to surveillance advertising is to buy contextual advertising, which allows advertisers to place ads where the consumers had already indicated interest in the content (such as ads for cooking classes on a recipes page).

Website and app owners can also use an Ad Choices icon that users can click on to learn why they are seeing an ad – or to opt out of the ads. Research has found that just having this Ad Choices icon on a website can foster digital trust.

Another best practice is to justify the data collection. Twitter, for instance, lets users know that it uses the information shared to show more relevant content and it also gives the user transparency and control of that information.

Growing awareness and concern about surveillance advertising will come with the recent Facebook whistle-blower incident.

Marketers need to rein themselves in before the legislation and public backlash catch up with them.

Aggressively placing creepy ads for Squid Game Halloween costumes after consumers have just completed a social media quiz is just going to turn consumers away in the long run and corrode the trust that consumers have in digital marketing.

stopinion@sph.com.sg

• Dr Chew Han Ei is senior research fellow at the Institute of Policy Studies, National University of Singapore, and a member of the Sunlight AfA (the Singapore Together Alliance for Action to tackle online harms, especially towards women)