Q&A on surveillance-based advertising

1. What is the definition of surveillance-based advertising?

We define surveillance-based advertising as digital ads that are based on tracking and profiling people. This includes advertising targeted at specific groups and individuals. The tracking and profiling can happen either on a platform, or across websites, apps, devices, and services.

2. If a ban is implemented, will there not be a negative impact on small and medium sized companies that rely on these types of ads? How can they now reach potential customers and what will happen to newspapers that depend on revenue from digital advertising?

We are not calling for a ban on advertising in general, only a subset of digital advertising. There are other ways of serving ads online that do not depend on tracking and profiling consumers. For example, a local business can still purchase ad space on the local news website, or a sporting goods store can advertise on websites for sports. It is also possible to show ads to visitors from different places based on "safe" data such as more general location (country, city), or consumers can be provided with active choices about topics that they would like to see ads for. In short, it is not a matter of hyper targeted ads based on surveillance versus random irrelevant ads.

3. Won't consumers prefer targeted ads if the option is to pay for services?

See above. That we have to choose between surveillance-based ads or paying for services is a false dichotomy. We are not proposing a ban on advertising as a way to fund online content. Advertising has existed for a very long time, while the surveillance-based advertising model has only become the norm during the last decade. It is time for businesses to return to less invasive advertising models. Both tech giants such as Google and smaller companies already have functionality for contextual advertising online.

4. Most advertisers use this marketing technology online, so is this a realistic proposal?

This is similar to arguments that have been made by corporations in response to calls to reduce emissions. We need advertisers and publishers to move away from the surveillance business model to level the playing field and foster healthier alternatives.

As we show in the report, there are serious doubts about the profitability of surveillance-based advertising in comparison to other models that are not based on tracking and profiling, but we understand that many companies are risk-averse and hesitant to change their business model or revenue streams. We hope that a ban would kickstart this transformation.

5. Shouldn't we let the GDPR do this work?

The GDPR should, at least in theory, be a safeguard from many types of tracking and profiling. Currently we have unfortunately not seen much enforcement on the subject of surveillance-based advertising, but this may change in the future.

However, as we describe in the report, there are many problematic issues with the surveillance business model that stretch beyond of the realm of data protection and privacy. Even if the worst privacy violations of the surveillance business model were solved, we believe that the business model is still harmful by facilitating disinformation, fraud, manipulation, discrimination, and more. Most of these issues would not go away if the tracking and profiling was done in a "privacy preserving" manner. Therefore, we need regulation that complements the GDPR.

6. Won't this proposal strengthen the platform power of Facebook and Google?

What we are proposing would also limit the ability of Facebook and Google to use consumer data to target ads. This could potentially help democratize the ad industry, which is already heavily dominated by Google and Facebook. For example, local newspapers will have the ability to sell ad space that is highly relevant to their local context. A ban on surveillance-based advertising may also spur new competitors in the ad market.

Of course a ban will not solve everything. There are serious issues regarding dominant actors and abuse of market power charges against these companies – for those issues we have competition regulation. We also want to see enforcement of data protection law that prevents these large companies from unlawful collection and use of personal data.

7. In the report, you argue that surveillance-based advertising is not effective, why should we then need a ban?

Even if the advertising is not as effective as many companies claim, the online advertising industry persists in using it. This allows data brokers to collect data about everyone. This is a serious violation of our privacy, and exposes us harms such as to manipulation and micro-targeted disinformation.

NATO has even claimed that data brokers are threat to national security. Furthermore, if you are discriminated against based on technology, it does not matter that the technology is wrong – it might even be worse.

8. Who is responsible for tracking and profiling consumers, and thus for complying to the ban?

All the actors that are involved share responsibility. Some of the large platforms (Google, to some degree Facebook) fulfill all of these roles, and have particular responsibilities. A ban would therefore necessarily lead to a significant overhaul of all parts of the digital advertising supply chain.

9. Which part of the process should be illegal? Collecting data, tracking users, analyzing data, using algorithms, sharing data across platforms, selecting target groups, exposing users to ads?

The collection, tracking, analyzing, and sharing of personal data for data processing purposes related to advertising, and exposing users to surveillance-based ads should be illegal.

10. Should all forms of tracking be banned? What about within a single platform?

Advertising based on user experiences in a service with actual transparency and consent is less problematic than widespread collection and sharing of data across services. Whether it should be a part of the ban and under what circumstances should be discussed. The current situation tends toward massive tracking all across the web, so a significant shift is needed before this becomes a real alternative.

11. **If selling/sharing data between companies is banned, will this not be a huge advantage for large platforms with a variety of services like Amazon, QQ, Apple etc? Or platforms who can base advertising on searches like Google?**

See question 6. A ban would need to be complemented by enforcement of competition regulation.

12. **Do advertisers purposely discriminate or manipulate consumers? What steps can they take to avoid it?**

We do not believe that most advertisers set out to discriminate or manipulate consumers. However, the tools of the surveillance-based advertising model make it easy to do so, creating an ethical race to the bottom, where problematic collection and use of personal data for advertising has become common. The automation of the technology also makes it hard to know whether a certain ad is shown (or not shown) to certain people based on discriminatory factors, and discrimination can be automated with little or no oversight.

13. **Is it really possible to separate surveillance-based advertising from contextual advertising**?

Yes. Contextual advertising is not based on data about you as a person, but relates to the context of what you are reading or watching. For example if you visited a news story about wine from Spain and saw an ad about travelling to Spain based on the text in the news story.

However, there are gray areas between the technologies, and contextual advertising models that involve tracking and profiling do exist. We do not want a shift that simply moves us from one type of commercial surveillance to another, so the suggested ban should also apply to contextual/ surveillance hybrid models.

14. **How is it possible to define whether sensitive personal data is used for marketing purposes**? (example: AI will rarely have a variable called “white male” but rather proxies likes country music, studied at certain schools, interest in cars etc)

A lot of information about us can be(come) personal data, and data-based advertising is problematic from a privacy point of view. As we point to in the report, there are many examples of surveillance-based advertising models using so-called proxy categories to circumvent protection of personal data (e.g. Facebook letting companies target based on “ethnic affinity”). This is one of the reasons why we propose a ban on advertising based on tracking and profiling – it is very difficult to know what data about an individual is “safe” when it can be combined with a lot of other data.

15. **If a ban happens, will consumers have to pay for content or to use platforms like Facebook, Google and Instagram**?

We do not believe that the major platforms would move to a subscription-based model. They can still show ads, and they will keep making money from advertising.

16. **Will increased use of active consent further desensitize consumers with regard to protecting their personal data**? (As can be argued has happened for cookie banners)

The rise of cookie banners and similar prompts have led to a consent fatigue, and the complexity of the data collection and sharing means that actual consent becomes an illusion. We believe that there is an urgent need to get away from this deluge of consent prompts. Moreover, these consent requests are meaningless, because there are no technical measures in place as part of the primary consent mechanism (IAB TCF) to prevent a person's data from being shared with parties they have said no to.

Therefore, rather than tweaking consent boxes, it is time to ban surveillance based advertising. With a ban, the need/pretext to collect our personal data will be significantly reduced, and we hope that can contribute to significantly less hassle with cookie banners and similar consent prompts. Simply put – if you don't collect personal data, you don't have to display a banner.

17. **What does the future look like with a ban on surveillance-based advertising? What will happen to the markets / what are the consequences of a ban**?

Online advertising will still exist, just not based on widespread collection and use of information about our every move. This is how advertising has functioned for a very long time. It can also level the playing field, and lay the groundwork for innovative solutions in advertising that does not depend on breaching the fundamental rights of consumers.

18. **What are the long term consequences of not banning surveillance-based advertising?**

The technology will become more efficient so that the discrimination and manipulation will be more subtle and therefore more efficient and prone to abuse. We will also see serious data breaches where our personal data, including location data, will be up for grabs and criminals will find new ways of using this for criminal purposes. We may also see more uses of the technology in attempts to subvert democratic elections, and other malevolent purposes. Furthermore, the race to the bottom will mean that publisher bottom lines may keep going down.

19. **My organization uses some of the tools described in the report. Will we still be able to reach relevant audiences?**

Yes, you can still advertise to relevant groups, just not based on information that is based on commercial surveillance. For example, you may be able to reach people interested in certain topics, or based in certain areas.

20. Don’t consumers actually like getting relevant advertising?

Many surveys and studies have shown that most consumers do not want companies to track and profile them. Many consumers find targeted ads creepy or annoying, and the prevalent use of ad blocking technology also indicates that a lot of consumers would prefer no ads at all. We are of course not calling for an advertising-free internet, and there are other ways of showing relevant ads.