global witness

BRIEFING March 2022

HOW FACEBOOK ENABLED ADVERTISERS TO TARGET USERS BASED ON THEIR MOST SENSITIVE CHARACTERISTICS

Sensitive data is amongst the most personal and invasive data that is collected and used by social media companies to serve users with ads. From information on your health or sexual preferences to your religious beliefs or political opinions, this type of targeting not only invades people's privacy, but also harms society as a whole. It can be weaponised by nefarious actors, manipulating vulnerable groups to distort democracy and public debate. Studies show it is also what citizens are most uncomfortable with. Despite limits set by the GDPR on when this data can be used, tech companies routinely profile and target users with ads based on their most intimate characteristics. At a time when the EU has an immediate opportunity to prohibit this type of targeting in the Digital Services Act, Global Witness reveals what the abuse of sensitive personal data looked like in practice on Facebook in Europe.

A week before Facebook announced it would be removing sensitive targeting options in January 2022, Global Witness was busy looking under the hood at Facebook to see how it was possible to target thousands of people in Europe with ads based on deeply personal data and inferences about them. What we found was disturbing, with targeting categories linked to religion, health, sexual orientation, and political beliefs available to anyone who wishes to advertise on Facebook including "Christian Views on Marriage", "Bone marrow and stem cell transplant survivors club", "Homosexuality", and "Being Conservative" (see Table 1).

In our previous communications with Facebook they claimed people's interest in a topic has nothing to do with their actual views, arguing: "People's interests are based on their activity on Facebook -- such as the pages they like and the ads they click on -- not their personal attributes." It is difficult to square this when one of Facebook's previous sensitive interest categories was explicitly about someone's views (i.e. "Christian views on marriage").

WHAT WE FOUND

We were able to successfully target a simple inoffensive ad to people in Europe using dozens of Facebook interest targeting options linked to sensitive data (see examples in Table 1). These ads were targeted at users in all EU Member States running for 24 hours with a £5 budget for each group category (political opinion, sexual orientation etc). For the category "Christian Views on Marriage" Facebook told us the estimated total audience size was 131,600-138,500 in all EU Member States, and in our time frame Facebook told us we reached 7,467 of them, costing us only £0.00064 for each person reached. There are serious questions that can be asked as to the accuracy of Facebook's targeting and whether it

is ever really reaching the intended audience, but the fact remained that it was possible to target people based on deeply personal information in a matter of a few clicks incredibly cheaply.

For the categories we found linked to religious beliefs Facebook estimated we could reach as many as 49 million users overall and 19,000 daily in the EU. For the interest category "pregnancy" Facebook had an estimated reach of as many as 400 million users and 19,000 daily.

TABLE 1: EXAMPLES OF FORMER FACEBOOK AD TARGETING - SENSITIVE DATA (NOV 2021)

Political Opinion	Religious Beliefs	Sexual Orientation	Health Information	Racial Or Ethnic Origin
Being Conservative	Protestantism	Homosexuality	Management of Crohn's disease	Latino culture
Right Wing News	Christian views on marriage	Same-sex marriage	Bone marrow and stem cell transplant survivors club	Hispanic culture
Christian Democratic Union Germany (DE)	Catholic Church	LGBT community	Pregnancy	African culture
Party of European Socialists	Judaism	Bisexual community	Fertility Friend (a fertility/ovulation app)	African diaspora culture
European People's Party	Hasidic Judaism	Transgenderism	Pregnancy and infant loss remembrance day	Chinese culture
The Greens - European Free Alliance	Islamic theology	LGBT+ Liberal Democrats		Non-resident Indian and person of Indian origin
Conservative Party (UK)	Buddhism	LGBT culture		
Labour Party (UK)	Church of England			
LGBT+ Liberal Democrats	Scientology			
Scottish National Party snp	Sikhism			

WHY THIS MATTERS

Regulatory gap: While Facebook changed its policy (potentially sensing regulatory headwinds), the problem still persists. As long as there is no legislation clearly prohibiting the use of sensitive data for advertising, what is to stop Facebook from changing its mind in the future and reintroducing these categories? What is to stop other social media companies from continuing or starting their own intricate systems of advertising based on people's sensitive data? We also don't know how Facebook's ad delivery algorithm probably still takes sensitive data into account when deciding who to show ads to.

EU citizens opposed: In 2021, Global Witness commissioned YouGov to gauge people's views in France and Germany on how their personal data is used to target them with ads. Overwhelmingly, people appeared deeply uncomfortable with targeting based on sensitive characteristics, and said that it shouldn't be possible to target based on health information (87%), who they voted for at the last election (84%), sexual orientation (81%), or religious views (81%). Another YouGov poll from earlier this year revealed that a majority of small business leaders also believe their customers would not be comfortable being targeted in this way, and think large online platforms – such as Facebook and Google – should face increased regulation of how they use personal data to target users while advertising online.

Democracy and national security: Beyond the clear rights breaches, the use of sensitive data for advertising also raises serious democracy and national security concerns. By segmenting the paid-for messages that are seen by specific groups of the electorate, dialogue between communities is prevented and disinformation can more easily thrive. This type of advertising can be weaponised by nefarious actors to distort public debate and influence democratic processes in Europe. This was never clearer than during the US 2016 election, which saw Russian interference via the Internet Research Agency who created fake Facebook accounts and issued more than $100,000 worth of targeted ads. These ads were on divisive issues such as race, gay rights, gun control and immigration. As part of this campaign, Black voters were encouraged to boycott the election. At a time when the world order is increasingly precarious and actors such as Russia seek to undermine the EU, the risks are now even higher.

DOESN'T GDPR ALREADY MAKE THIS ILLEGAL?

The way an online platform analyses people's personal data to make inferences about their interests and segments and atomises them into audiences is data processing is covered by the GDPR. Article 9 of the GDPR prohibits the processing of personal data revealing "*racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*", except in limited circumstances such as when the data subject has given explicit consent.

Despite the GDPR setting high standards for how this consent should be given – that it should be freely given, specific, informed and unambiguous - platforms and ad tech giants have not seen this as an impediment to continuing to profile and serve users with ads based on their sensitive data.

When Facebook announced its policy change on sensitive ad targeting, it did not say this was because of data protection rules but rather that they had "heard concerns from experts that targeting options like these could be used in ways that lead to negative experiences for people in underrepresented groups." As such, there continues to be a regulatory gap in Europe for protecting people's sensitive data.

THE DSA

The Digital Services Act (DSA) offers an immediate opportunity to set **a clear prohibition** on this practice for very large online platforms, addressing systemic risks within the current system and adding new vital safeguards for the protection of people's fundamental rights. This is surveillance that people never asked for, nor meaningfully consented to. The risk of inaction goes beyond rights breaches and includes very live national security and democratic interference threats – when nefarious actors weaponise these tools against us.

Importantly, for the prohibition on sensitive data to be effective it must include **inferred data**. Online platforms use sophisticated machine learning models to infer highly sensitive information about their users. These predictions are based on seemingly benign data such as search history, which on their own do not reveal sensitive data. However, when this data is combined revealing a specific behavioural pattern it enables ad targeting that exploits vulnerability (e.g. a user's fears, hidden political sympathies, ideological bias).

We strongly urge European legislators to back the European Parliament's position to ban the use of sensitive data for advertising purposes in the DSA.