Does Facebook Use Sensitive Data for Advertising Purposes?

Citizens worldwide have demonstrated serious concerns regarding the management of personal information by online services. For instance, the 2015 Eurobarometer about data protection reveals that: 63% of citizens within the Eurpean Union (EU) do not trust online businesses, more than half do not like providing personal information in return for free services, and 53% do not like that Internet companies use their personal information in tailored advertising. Similarly, a recent survey carried out among U.S. users reveals that 53% of respondents were against receiving tailored ads from the information websites and apps learn about them, 42% do not think websites care about using users data securely and responsibly at all, and 73% considers websites know too much about users. A survey conducted by Internet Society (ISOC) in the Asia-Pacific region in 2016disclosed that 59% of the respondent did not feel their privacy is sufficiently protected when using the Internet, and 45% considered getting the attention of policymakers in their country on data protection a matter or urgency.

Policymakers have reacted to this situation by passing or proposing new regulations in the area of privacy and/or data protection. For instance, in May 2018, the EU enforced the General Data Protection Regulation (GDPR) across all 28 member states. Similarly, in June 2018, California passed the California Consumer Privacy Act, which is claimed to be the nation's toughest data privacy law. In countries like Argentina or Chile, the governments proposed new bills in 2017 updating their existing data protection regulation. For this article, we will take as reference the GDPR since it is the one affecting more countries, citizens, and companies.

The GDPR (but also most data protection regulations) define some categories of personal data as sensitive and prohibits processing them with limited exceptions (for example, the user provides explicit consent to process that sensitive data for a specific purpose). In particular, the GDPR defines as sensitive personal data as: "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."

In a recent work, we demonstrated that Facebook (FB) labels 73% of users within the EU with potentially sensitive interests (referred to as ad preferences as well), which may contravene the GDPR. FB assigns user's different ad preferences based on their online activity within this social network. Advertisers running ad campaigns can target groups of users that have been assigned a particular ad preference (for example, target FB users interested in Starbucks). Some of these ad preferences may suggest political opinions (for example, Socialist party), sexual orientation (for example, homosexuality), personal health issues (for example, breast cancer awareness), and other potentially sensitive attributes. In the vast majority of the cases, the referred sensitive ad preferences are inferred from the user behavior in FB without obtaining explicit consent from the user. Then advertisers may reach FB users based on ad preferences tightly linked to sensitive information. For instance, one of the authors of this article received the ad shown in the figure below(left side). The text in the ad clearly reflects the ad was targeting homosexual people. The author had not explicitly defined his sexual orientation, but he discovered that FB had assigned him the "Homosexuality" ad preference.