For immediate release

13 September 2023

Disinformation Project discovers invasive tracking technology used by New Zealand political parties, raising concerns about privacy and ethics ahead of the election.

Independent research group The Disinformation Project is concerned about the use of invasive user tracking and micro-targeting technology by four major political parties ahead of the 2023 General Election.

The group has discovered that the official websites of Labour, National, ACT, and the Green Party use Facebook Pixel without disclosure or user consent, to track all visitors.

Pixel-tracking technology, like Facebook Pixel, follows a website's visitors across other websites and even mobile apps, recording and sharing their information, interests, and behaviour.

"This type of technology being used by political parties is unprecedented in our electoral history. New Zealanders have a basic right to know how their data is being used, and this is especially important when trust and integrity are key electoral issues," says The Disinformation Project's Founder and Director, Kate Hannah.

The Project is especially concerned that pixel-tracking is not made obvious to website users and is hard for people to opt out of.

Facebook's parent company, Meta, states websites that use pixels are required to feature:

> *"…a clear and prominent notice on each web page where our pixels are used that links to a clear explanation that third parties, including Meta, may use cookies, web beacons, and other storage technologies to collect or receive information from your websites and elsewhere on the Internet, and use that information to provide measurement services, target and deliver ads"*

The Disinformation Project found that none of the four political party's websites have done this. While all parties have a privacy policy on their website, none of these policies mention the use of Facebook Pixel to track visitors.

Pixel-tracking enables the tracking and targeting of users based on their behaviours, interests, interactions, race, ethnicity, location, and other factors. This sophisticated targeted advertising enables the creation of audience groups to either target or exclude, and can be discriminatory by design.

The Disinformation Project is flagging that the creation of micro-targeted groups can contribute to increased social division and the spread of disinformation. For example, the segmentation of target audiences diminishes the ability of media and researchers

to openly document, and debate claims made by each of the four parties, especially in the context of a general election.

Harms arising from micro-targeting have been studied across multiple countries and contexts, such as the Facebook-Cambridge Analytica data scandal, revealed in 2018.

The Disinformation Project's Research Director, Dr Sanjana Hattotuwa says the use of Facebook Pixel technology by four of the country's leading political parties is deeply concerning.

"This technology benefits those with the most amount of money to spend on targeted campaigns, making pixel-tracking during an election potentially undemocratic. We are concerned that this technology enables political parties to target very specific voter groups and spread false information with very little oversight. An example would be targeting supporters of an opposing party with false information about that party,"

"The use of this technology impacts everyone eligible to vote, no matter who they support, and vote for," says Dr Hattotuwa.

The Disinformation Project believes the use of pixel-tracking by political parties in Aotearoa may breach the New Zealand Privacy Act (2020) which mandates that organisations must transparently disclose to individuals how their personal data will be used.

Pixel-tracking can also expose people's personal details, including health information like gender identity, pregnancy, and mental health issues. Earlier this year, several NHS trusts in the UK were reported to have used Facebook Pixel to share sensitive patient data, impacting millions of people.

"Even if the use of pixel-tracking without disclosure by political parties was due to an oversight, rather than deliberate covert use, this is a concerning issue - particularly in the context of the General Election," says Hannah.

"We are urging political parties to urgently reconsider their use of these technologies. And if they choose to continue to do so, they must offer visitors clear visibility on the use of Facebook Pixel, and instructions on how to opt-out."

The Disinformation Project has notified the Office of the Privacy Commissioner and the Electoral Commission of its concerns over pixel-tracking, as well as directly contacting the head offices of Labour, National, ACT and the Green Party.

ENDS

Contact

media@thedisinfoproject.org

FURTHER DETAIL

Meta describes Facebook Pixel as “a piece of code for your website that lets you measure, optimise and build audiences for your advertising campaigns”.

Tracking technologies like Facebook Pixel are designed to be used in conjunction with personalised targeting of users across the web, and Meta’s own products and apps.

The Disinformation Project is also concerned with the wider adoption, adaptation and potential adversarial use of pixel-tracking technology by disinformation producers on Facebook, using templates established by the country’s leading political parties.

While Facebook allows users to opt-out of pixel-based targeting, this is a difficult process, and many people are unaware they are subject to intrusive tracking in the first place. This also has a significant impact on data sovereignty, particularly Māori data sovereignty.

The Disinformation Project believes that pixel technology-based tracking of users is inherently problematic, particularly in the context of polls, and propaganda. The use of this technology during a general election campaign raises urgent questions on whether existing laws and guidelines about voter privacy are fit for purpose.

The Project also believes Meta should provide more granular details on their Ad Library platforms to better highlight the use of detailed targeting, custom audiences, and lookalike audiences.

Specifically, the Project believes that tools for advertisers, especially political parties or candidates, must allow for independent scrutiny and audits.

INTERNATIONAL CONTEXT

The UK’s Information Commissioner’s guidance on political campaigning online has pointed out concerns about the use of tools that enable the creation of so-called ‘look-alike’ and ‘custom’ audiences, noting that “the use of lookalike audiences should be made transparent to the individuals”, and that “if individuals have objected to the use of their personal data for marketing purposes, you also need to ensure that you do not use their data for the creation of a ‘lookalike’ audience.”

Pixel-tracking technologies have contributed internationally to the acceleration of ‘affective polarisation’ or increasing social division. Cambridge Analytica is a cautionary example of the use of micro-targeting to shape important public conversations, including elections.

The Austrian Data Protection Authority ruled that pixel-tracking technologies, such as Facebook Pixel, violated the European Union’s General Data Protection Regulation (GDPR). This means that websites of four leading political parties in Aotearoa New Zealand New Zealand using Facebook Pixel may also be contravening GDPR for individuals based in the European Union, including expatriate New Zealand citizens.