

EU citizens being tracked on sensitive government sites

Researchers find advertising monitors on official pages of 25 member states



© Getty





MARCH 18, 2019

EU governments are allowing more than 100 advertising companies, including Google and [Facebook](#), to surreptitiously track citizens across sensitive public sector websites, in apparent violation of their own EU data protection rules, a study has found.

Danish browser-analysis company Cookiebot found ad trackers — which log users' locations, devices and browsing behaviours for advertisers — on the official government websites of 25 EU member states. The [French government](#) had the highest number of ad trackers on its site, with 52 different companies tracking users' behaviour.

Google, YouTube and DoubleClick, Google's advertising platform, accounted for three of the top five tracking domains on 22 of the main government websites.

Researchers also studied the websites for EU public health services, finding that people seeking health advice on sensitive topics such as abortion, HIV and mental illness were met with commercial ad trackers on more than half of the sites analysed.

Nearly three-quarters of the 15 pages scanned on the Irish health service website contained ad trackers, while 21 different companies were monitoring a single French government webpage about [abortion services](#). Sixty-three trackers monitored a

single [German webpage](#) about maternity leave. Google DoubleClick trackers were found on health pages providing information on [HIV symptoms](#), [schizophrenia](#) and [alcoholism](#).

Researchers also found that while many governments mentioned Google analytics cookies, which are used to run the website, in their privacy policies, they did not disclose any advertising-related cookies.

“

It shows how pervasive and broken online ad tracking remains, and how urgently we need to fix it

Diego Naranjo, European Digital Rights

“Any website has a responsibility to inform their user about any data collection and processing happening on their website,” said Eliot Bendinelli, a technologist at Privacy International, the non-profit. “The fact that these websites . . . can’t comply with this basic requirement shows that the current tracking ecosystem is out of control.”

Many commercial trackers appeared to be gaining access to these public websites through backdoor tactics, including via social sharing widgets, such as ShareThis.

“We found a lot of adtech trackers were smuggling in other third parties through these plug-ins, without the consent of users or knowledge of the governments themselves,” said Daniel Johannsen,

chief executive of Cookiebot. “Although the governments presumably do not control or benefit from the documented data collection, they still allow the . . . privacy of their citizens to be compromised, in violation of the laws that they have themselves put in place.”

Industry experts say the personal data that adtech companies are harvesting from visitors to EU government sites could be combined with data from other sources to draw [detailed profiles](#) of each unique user — which could in turn be sold to data brokers.

“Browsing histories are very intimate information. They show what we’re worried about, what our plans are, what we are interested in, our daily routines, the focus of our work,” Mr Bendinelli said.

“Government websites are . . . a case that’s especially concerning. They offer crucial information and services that people depend on and often can’t choose not to use.”

Diego Naranjo, senior policy adviser at the civil rights organisation European Digital Rights in Brussels, said Cookiebot’s findings raised questions about whether the public websites were in violation of the EU-wide General Data Protection Regulation, which went into effect last year.

“We need an analysis from EU data protection officers of how this behaviour is in line with GDPR,” he said. “It’s not obvious to me how this is based on any legal grounds . . . It shows how pervasive and

broken online ad tracking remains, and how urgently we need to fix it.”

Google said: “Our policies are clear: if website publishers choose to use Google web or advertising products, they must obtain consent for cookies associated with those products.” They added that Google did not permit publishers to “build targeting lists based on users’ sensitive information, including health conditions like pregnancy or HIV”.

A Facebook spokesperson said the investigation “highlights websites that have chosen to use Facebook’s Business Tools, for example, the Like and Share buttons, or the Facebook pixel”.

“Our Business Tools help websites and apps grow their communities or better understand how people use their services,” they added. “Facebook considers it the responsibility of the website owner to inform users of which companies may be tracking them.”