Source : www.thehindu.com Date : 2022-01-11

FOLLOWING THE TRAIL OF CRUMBS

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

On January 6, Google and Facebook were hit with a combined 210 million Euros fine for not complying with France's data privacy law. The country's data protection authority, CNIL, said that Facebook, Google's French homepage and YouTube websites failed to provide its users a 'disable' cookies option similar to the enable button.

The authority said these websites made it hard for users to refuse cookies and nudged them to accept it. They required users to make several clicks and take a circuitous route to disable cookies, which affects the website visitor's freedom of consent on the Internet.

A user expects to be able to quickly check a website, and the fact that they can't refuse cookies as easily as they can accept them influences their choice in favour of consent, the data privacy watchdog noted.

Cookies and web beacons are electronic placeholders that are kept on your device by websites to track your specific movements on that website over time. They are useful to a limited extent to individual users. For example, cookies retain login details for quick retrieval next time the user logs back in. But they also extensively track people's digital footprint and share browsing details with advertisers.

HTTP cookies, or Internet cookies, have become an essential fixture of the modern Internet, and are a necessary part of web browsing. For developers, this tracking tool is a way to customise and personalise their interface for users. But they pose a threat to user privacy.

Using cookies, websites remember you, your login credentials, browsing history, and sometimes peep into your e-commerce shopping carts. The data these cookies gather is largely used by advertisers and marketers to place and sell their products online.

Most cookies are perfectly safe, and are generated by the websites themselves to enhance their page's performance. These are usually harmless, and are commonly called necessary cookies.

Third-party cookies are more troubling as they are placed by companies that do not own the website the user is accessing. For example, a student may be surfing an educational website that contains advertisements of various other companies. These advertisers can deploy relevant cookies to track the user's digital footprint.

But what happened in the case of Google and Facebook is related to first-party cookies. And it was also a matter of how large platforms make it hard for its users to deny tracking. This was at the heart of the of 210 million Euros CNIL fine.

While complaints against Facebook and Google over similarly problematic consent issues continue to languish at the Irish Data Protection Commission (DPC), France has taken a step forward and set a precedent.

The CNIL's action is based on a piece of EU legislation, the ePrivacy Directive, which gives France a creative way to apply General Data Protection Regulation (GDPR) standards within its borders. According to Article 82 of the French Data Protection Act, any subscriber or user who uses Internet-based service must be informed in a clear and comprehensive manner by the controller or their representative of the purpose of any action to access information already

stored in the user's electronic device. They should also seek consent from the user to record information in such a device. The controller is also obligated to provide means to oppose such interference. Under Article 6 of GDPR, if consent is the legal basis for claiming to process users' data, then it must be informed, specific and freely given in order for it to be obtained legally.

For Google, this is the second time the company is fined by CNIL in less than a month. In December 2020, the search giant was fined 100 million Euros by the French regulator for dropping tracking cookies without getting consent from users.

India, like France, should draft rules to protect its citizens from being stalked by large tech firms, which control a significant part of the digital space. But, the country has no comprehensive personal data protection at the moment.

While some experts note that the use of cookies without the user's consent could be subsumed under Section 43 of the Information Technology Act, in the absence of any explicit legislation, companies can circumvent the law by finding technical loopholes. For instance, the Section deals with a 'computer virus' that can potentially contaminate an electronic device. But cookies don't harm the computer like the malware.

The draft Personal Data Protection Bill (PDP), 2019, which is likely to be passed by the Parliament during the Budget session is also not up to the mark on regulating cookies.

The Bill defines 'personal data' as any information about a natural person who can be directly or indirectly identified. This means, businesses that use cookies can argue that their web trackers inherently cannot spot a 'natural' person.

Perhaps where the PDP Bill can help is with its definition of 'personal information', which can be used to trace a natural person. And this is what cookies do for the businesses that deploy them.

The chips are Intel's first effort in many years in the market and will take on leader Nvidia, which had graphics chips sales of $9.8 billion in its most recent fiscal year, a 29% increase.

The concept car uses less than 10 kWh of electrical energy to travel 100 km. When translated into fossil-fuel consumption, this is around 1 litre per 100 km.

END