Exposing alarming practices of online tracking on websites and apps

March 4 2022

Credit: Unsplash/CC0 Public Domain

Researchers are calling for website and app developers to be more transparent and to educate users about online tracking practices, after a study has shown cookie notices and user opt-out routes violations in 97

out of EU's 100 most popular websites. The study also reveals that the corresponding Android apps of such popular websites suffer from the same non-complaint practices.

Led by Dr. Maryam Mehrnezhad, Lecturer in Cybersecurity and Privacy at Newcastle University's School of Computing, the research team observed the top 100 EU websites from a user's point of view to analyze how these websites use and present privacy-enhancing technologies (PETs).

Publishing their findings in the journal *Proceedings on Privacy Enhancing Technologies* and the European Workshop on Usable Security, the scientists found that only three websites allowed users to reject cookie notices as easily as they could accept. This means that the practices of the other 97 websites are non-compliant with the law and do not meet the minimum requirements provided by the GDPR.

The study also shows that it would take an overage of three clicks for the user can opt out of the cookie notice on a website, and six clicks on average if the user accepts the cookie notice but later decides to opt out.

Intrusive online tracking

Dr. Mehrnezhad said: "Recognizing the users' mindset is the key for multiple stakeholders such as developers and policymakers to protect them from online tracking across platforms e.g. websites, apps and IoT devices. That is why we have conducted our studies from a non-expert user's point of view."

Study co-author, Dr. Ehsan Toreini, Assistant Professor at Durham University, added: "Intrusive online tracking has gone to a different level now. For instance, even in the presence of the recent data protection regulations, now advertising companies have an individual profile per

user allowing them to track each user individually."

Co-author Dr. Kovila Coopamootoo, Lecturer (Assistant Professor) at King's College London, said: "Notice and consent choices need to be fair and usable and not be the users' burden."

Online tracking enables online services companies to collect data, which for example could be used for personalized offers. Any device connected to a network can leak data about its users and environment. The most common tracking method is known as cookies—small pieces of data (in text form) that are downloaded to a device when a website is visited. Other tracking methods include websites creating a fingerprint of the user's browser with information collected through JavaScript.

To mitigate these issues, the study authors recommend that designers and privacy educators need to not only provide information, but to guide different user groups according to their preferences, and support accessibility of PETs within users' preferred route. The team highlights that regulators should identify those needs leading to more effective and sometimes distinctive regulations.

More information: Maryam Mehrnezhad et al, How Can and Would People Protect From Online Tracking?, *Proceedings on Privacy Enhancing Technologies* (2021). DOI: 10.2478/popets-2022-0006

Maryam Mehrnezhad, A Cross-Platform Evaluation of Privacy Notices and Tracking Practices, *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (2020). DOI: 10.1109/EuroSPW51379.2020.00023