Can anyone be completely anonymous?

December 3 2019, by David Bradley

Credit: CC0 Public Domain

Research published in the *International Journal of Electronic Governance* has investigated whether any of five "anonymous" social media applications are secure in that they do not allow a third party to see personal data or track the users.

Vasileios Chatzistefanou and Konstantinos Limniotis of the Open University of Cyprus, explain how anonymization of personal data should protect user privacy from data mining and data publishing systems. However, this may well not always be the case. Indeed, removing personal identifiers does not ensure privacy as there are techniques that can easily be employed to build a unique fingerprint based on the characteristics of the data itself, which then be used to home in on the identity of a user with or without additional information.

It has been known for a long time that three pieces of information—birth date, sex and zip code—can be used to identify 87 percent of the US population. Moreover, if such information is not available to another party wishing to de-anonymize activity on a given device or in an application, then data points such as identity mobile subscriber identity (IMSI), media access control (MAC) address, International Mobile Equipment Identity (IMEI), Android ID, Google Advertising ID (GAID), and so on, can be used to focus on what is essentially a unique fingerprint for a given device and thence perhaps the user. Anonymity cannot be guaranteed, it seems within any system or application regardless of promises and regardless of regulations, such as General Data Protection Regulation (GDPR) for citizens of the European Union (EU).

Fundamentally, "Our analysis concludes that there is personal data processing in place even in so-called anonymous applications which in turn implies that a user's anonymity cannot be ensured, whilst the corresponding privacy policies may leave room for further improvement," the team writes.

Provided by Inderscience