International Bar Association
the global voice of the legal profession

Dear Friends,

Hope you are having a relaxed break in most parts of the world. For me, July had a major focus on public speaking on topics related to privacy, the last being on the twin concepts of ‘Pseudonymisation’ and ‘Anonymisation.’

As I understand, General Data Protection Regulation (GDPR) defines ‘pseudonymisation’ as “the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable individual.” This type of data may enjoy fewer processing restrictions under GDPR, which protects data privacy across the European Union (EU). ‘Anonymisation’, on the other hand, is the process of permanently removing personal identifiers, both direct and indirect, which may lead to an individual being identified. India is considering the definition of ‘anonymisation’ as “…such irreversible process of transforming or converting personal data to a form in which a data principle cannot be identified, which meets the standards of irreversibility specified by the Authority.” The biggest concern raised in the context of anonymisation of data is its de-anonymisation, which is the process of using information from different data sets to re-create the anonymised data.

I am sure my EU colleagues will be able to elaborate much better than me. Nonetheless, I will share some insights from my panel discussions. The fundamental theme was that reducing re-identification risk can impact analytical usefulness.

As with all privacy-enhancing technologies (PET), the degree of privacy protection added to a dataset affects the analytical utility of the resulting dataset. Obscuring the true value of a field reduces both the ways in which it can be used for analytics and the precision of the analytical outputs. Today’s data-driven world has datasets with many billions or trillions of records. Human intuition or expertise alone cannot decide which transformations to apply as part of a pseudonymisation. It is likely that there will be either unacceptable levels of residual privacy risk or destruction of analytical usefulness of the data.

The privacy-utility trade-off makes it impossible to completely mitigate all potential re-identification attacks, which necessitates a risk-based decision about the use of data. Implementing the privacy-by-design principle offers a solution here.

While we often hear the terms used interchangeably or imprecisely, pseudonymisation is not equal to anonymisation. Interestingly, in some cases, protecting pseudonymised data by placing it in a controlled environment reduces re-identification risk to the extent that the data is considered anonymous! So, by varying environmental controls, the same data may be considered pseudonymised in one environment, but anonymous in another.

With 1.7 megabytes of new data being created every second, it is burdensome for organisations to adequately protect personal information, especially sensitive personal information. The Internet of Things (IoT) is certainly a major area of concern for all security professionals, given that IoT vendors do not proactively release security vulnerability patches for connected devices, yet the number of devices is growing at an unimaginable pace. Then come the BYOD policies that allow employees to bring their own devices to the workplace. Monitoring networks with Intrusion detection systems and Intrusion prevention systems (IDS/IPS), SIEM (Security Information and Event Management) tools, as well as any other advanced security analytics, have become essential in finding malicious activity in the network, applications, and data.

Now to the most relevant datapoint for all of you – IBA's Annual Conference 2022. Do register for the same **here** and try to attend the special programming that your committee is putting together for you.

Warm regards,

Sajai Singh

Chair, IBA Technology Law Committee