Twitter Thread by Kenna Partners

Kenna Partners
@Kenna_Partners

We are live!

> Our Social Media Discussions are Back!
>
> Today our topic is: Digital Identity and the Law
>
> Join the Conversation on Twitter by 5PM! pic.twitter.com/TbbqMMQbLc
>
> — Kenna Partners (@Kenna_Partners) January 13, 2021

Good evening everyone! Welcome to the Year 2021 and the first KP Social Media Discussion of the year. Today we are gonna discuss the concept of digital identity and the legal issues it raises.

It is not news that the fourth industrial revolution has led to many novel innovations on how everyone lives their lives.

Most operations in life can now be done digitally since the rise of the digital age and social networking, and since the Corona Virus mandated lockdowns most social interactions from work to school to parties, weddings and funerals are done digitally.

In Nigeria, there is a ramped up pressure to create a digital profile for every Nigerian through the National Identity Card Scheme which is now operated by the Federal Ministry of Communications and Digital Economy.

The end result is most individuals who use any of these applications fairly often have built a digital profile of sorts which has all their perceived likes and dislikes, patterns, personal details, medical details, physical details, financial details, political affiliations...

and ideologies, location and many of the other details that make up that individual.

This information is known as the digital identity of a person, and this discussion is going to analyse the few legal issues that have arisen as a result of the discovery of the digital identity and raise suggestions for the protection of one's digital identity.

What is one's digital identity?
The digital identity is the body of information about that individual, organisation or electronic device that exists on the internet or on any other digital framework.

It is created by unique identifiers and user patterns which make it possible to detect individuals or their devices, and it often includes:
1.The collective aspect of the set of characteristics by which a thing is definitively recognisable or known.

2.The set of behavioural or personal characteristics by which an individual is recognisable as a group member.

3.The distinct personality of an individual regarded as a persisting entity; individuality

4.Information, such as an identification number, used to establish or prove a person's individuality.

Generally, the information generated through one's digital identity is often so accurate that it can read patterns enough to identify what products the individual will be interested in purchasing, the political leaning of the individual in any particular election

In some cases, it can determine when an individual is even pregnant before the person even knows it. This information oftentimes is the type of knowledge about a person that is generally kept close to one's heart,

and now it is collected oftentimes without the user knowing it has been collected or understanding what exactly has been collected. The end result is a situation where ones' digital information is available for sale to the highest bidder without one's knowledge.

Legal Issues Digital Identity Raises
Discrimination
Many believe that the use of digital identities would reduce issues of discrimination, unfortunately, due to the fact that even the person who designs the digital platforms has perceived biases one can surmise that

technology alone cannot protect human rights or prevent discrimination. Studies from the World Bank have concluded that digital identity technologies may often unintentionally impede on the rights of those that they intend to benefit.

These technologies can simultaneously include and exclude individuals from protection. For instance, Blockchain technology which was used to identify highly persecuted groups of people such as the Rohingya minority in Myanmar and allow them to access services in

a host country such as Bangladesh may also allow for more efficient ways to discriminate these populations since identification makes them more visible

Another instance is the marginalisation of ethnic minorities such as the Uyghurs in China, where it was alleged that their digital profiles were used to identify them for arrest.

In another aspect of discrimination, it has been shown that biometric data collected from older individuals are often of less good quality. This is because ageing and manual labour have caused changes aged peoples biometric information.

Sole reliance on biometric technology for identification and verification purposes can, therefore, affect older individuals harshly, as their thumbprints and iris scans may not be accurate enough to guarantee verification and identification will always be possible.

As a result of this, they may experience obstacles in joining and using digital identity programmes.

There is also the problem of facial recognition software, which is often used by law enforcement to identify suspects mixing up the faces and identities of black people, often to devastating effect. This is often caused by the person who programmed the facial recognition software

not using enough black faces to test run the algorithm that identifies faces, as a result, the algorithm identifies multiple black people as the same person

Finally, there have been incidences of individuals being targeted on the basis of their perceived political affiliation as a result of the data obtained from their aggregated digital profile

Digital Privacy
It has now been decided that one's right to private life encompasses one's 'personal identity,' 'aspects of physical and social identity a person's right to their image and personal data, including biometric, genetic and electronic data in EU countries.

State interferences with this right can only be justified if they have a legal basis in domestic law, pursue a legitimate aim and are necessary and proportionate to that aim. The question now is what is the legal protection if this private life is infringed by a business?

As in the case of targeted advertisements or in the case where one is targeted by their perceived political beliefs from analysis of the individuals' digital data.

In the case of state intervention, domestic policies establishing and managing digital identity programmes must determine with enough clarity their scope of application, the safeguards they put in place on data storage, duration, usage, destruction and access of third parties,

as well as the guarantees against arbitrariness and abuse. To illustrate, the Supreme Court of India recently confirmed that these requirements applied to India's Aadhaar programme, which had been criticised for lacking a comprehensive privacy safeguard mechanism.

This case may eventually become instructive in Nigeria as there are rumours that most of the data collected by government agencies are for sale on the dark internet. Domestic laws ought to require that technology developers implement such safeguards as a matter of design.

Public-private initiatives led by non-state actors, including private companies, should align their practices to the existing standards on privacy and data protection.

In this regard, data protection rules provided by the GDPR and NDPR can be of assistance. These rules apply to state and non-state actors alike, even though formally their extraterritorial reach is limited to processing or controlling of EU/ Nigerian data subjects' personal data

Finally, there is the issue of the expansion of digital personality to include the right of an individual to be represented digitally this will include the addition of the right to access of the internet as well as the right to utilise one's freedom of speech, and expression

on the internet. It must be noted, that these perceived rights are untested and thus must be first tested in court and recognised in municipal and then international law and treaties before it can become established.

Another question that has been asked is how the right to be forgotten balances with the new Government drive for smart/ digital identification. It is our belief that if the Government's digital identification is backed by law that it will supersede the individuals right to be

forgotten.

In conclusion, while new technologies can revolutionise how individuals are identified and how the information about the individual is collected used online, they must also be used ethically and legally within the bounds of the law and best practices.

However, emerging digital identity platforms will only effectively contribute to protecting human and digital rights if they comply with the legal framework and that if that framework is tested regularly in Court.

This will adequately mitigate the risks of potential discrimination, and promote high standards of privacy and data protection. Such considerations should be integrated into digital identity platforms' design from the outset.

In Nigeria, it's proposed we build a secure, locally hosted Cloud service to hold all the Federal Data being collected. It is also advised that innovators and technology developers promote best practices and contribute to the implementation of better levels of protection of human

rights around the world Maybe through the creation of a developer ethical code of conduct of sorts. Their actions in this field would thus ensure that human rights remain relevant amid the rapid technological advances that have come to define our current digital age.

This brings us to the end of our discussion. Thank you for joining us! We hope to see you at our next discussion in a fortnight.

@threadreaderapp unroll please