Contributions from MAURITIUS.

1. Recent developments in national or regional legislation, case law, and practice concerning the right to privacy in the digital age.

The right to privacy is a fundamental human right recognised in Mauritius. The Data Protection Act (DPA) is the law which governs the protection of personal data. In 2009, the Government of Mauritius established the Data Protection Office. The office acts with complete independence and impartiality and shall not be subject to the control or direction of any other person or authority in the discharge of its functions under the Act. The Data Protection Commissioner is responsible for upholding the rights of individuals set forth in the DPA and for enforcing the obligations imposed upon controllers and processors. In 17 June 2016, Mauritius acceded to the Council of Europe's Convention for Protection of Individuals with regard to Automatic Processing of Personal Data commonly known as Convention 108. The convention is the first and only international legally binding instrument dealing explicitly with data protection and Mauritius became the second non-European state after Uruguay to sign the convention which entered into force on 1 October 2016 in Mauritius.

In 2017, the Data Protection Act 2004 was replaced by a new and more appropriate legislation known as the Data Protection Act 2017 which came into force on 15 January 2018 in Mauritius. The new DPA aims at strengthening the control and personal autonomy of data subjects over their personal data, thereby contributing to respect for their human rights and fundamental freedoms, in particular their right to privacy, in line with current relevant international standards, in particular the European Union's Regulation on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, commonly known as the General Data Protection Regulation (GDPR).

The functions of the Data Protection Commissioner are defined under section 5 of the Data Protection Act 2017 and include:

(a) compliance with this Act and any regulations made under it;

(d) control on all data processing operations, either of his own motion or at the request of a data subject, and verify whether the processing of data is done in accordance with this Act;

(h) undertaking research into, and monitor developments in, data processing, and ensure that there is no significant risk or adverse effect of any developments on the privacy of individuals;

(i) examining any proposal for automated decision making or data linkage that may involve an interference with, or may otherwise have an adverse effect, on the privacy of individuals and ensure that any adverse effect of the proposal on the privacy of individuals is minimised;

2. Surveillance and communication interception.

In general, the Criminal Code allows a judge or magistrate to authorise the interception of private communications in limited circumstances where the enforcement agency for example the Police department has made an application for such warrant.

In 2011 the Information and Communication Technologies Authority (ICTA) put in place an Online Content Filtering (OCF) mechanism to filter access to Child Sexual Abuse (CSA) sites should Internet users in Mauritius attempt to gain access to such sites. The OCF system enlists the collaboration of Internet Service Providers. The statistics as to how many CSA sites have been accessed and filtered are available in the ICT Observatory section on the Authority's website (http://www.icta.mu/stats_cyber.html) As at September 2013 there were some 24 thousand attempts to access CSA websites by Internet users in Mauritius.

The portal launched today goes a step further since it will enable Mauritian citizens to be proactive and to themselves report CSA sites or illegal content they may inadvertently come across whilst they are legitimately using the Internet. The ICTA wishes to make the Internet a safer place for children and young people who are increasingly interacting in cyberspace.

Source https://www.icta.mu/

Sometimes, companies (controllers) use global position system (GPS) in their vehicles for the monitoring of their vehicles. Controllers have to ensure that they have complied with their obligations of informing parties(employees) concerned of the use of GPS and that they are using it for lawful purposes. The conditions for lawful purposes are defined in section 28 of the Data Protection Act 2017.Whenever consent is required they have to ensure they have obtained that consent and the whole mechanism of managing consent is in place.

In Mauritian IT laws, there are no provisions for surveillance of the citizen's communication. Bulk data is not collected and processed for any specific information of an individual. Targeted ICT systems intrusions are not automated and access to personal data is an offence without the consent as per the DPA 2017.

3. Encryption and anonymity as enables for the enjoyment of human rights, including the right to freedom of expression and of opinion; challenges raised by encryption and anonymity and ways to address these challenges.

Encryption and anonymity have entered the lexicon of privacy, since individuals are seeking to preserve their own private sphere online.

Encryption as per Data Protection Act 2017.

The Data Protection Act (DPA) 2017 defines encryption as the process of transforming data into coded form. In other words, encryption of personal data is a data security technique which has the effect of rendering data unintelligible to any person who is not authorised to access it due to encoding the information, so that only parties with access to a decoding mechanism and a secret decryption key can access the information.
According to Section 31 2 (a) of the DPA 2017, encryption is regarded as an appropriate technical and organisational measure to ensure the security of processing.

Encryption of data is one of the promising solutions in order to ensure privacy, particularly in cloud computing environments. When a controller encrypts the data before uploading it to a cloud, the data is regarded as personal data for the controller who holds the decryption key and the controller thus remains accountable for the data.

As encrypted personal data makes sure that no unauthorised person is able to use the personal data, only the original data controller is able to identify the persons related to data stored in the cloud – and not the cloud operator nor third persons. Hence, encryption may serve as a tool to safeguard data protection. Furthermore, when processing is carried out on behalf of the controller, such as in a cloud computing scenario, the DPA 2017 introduces several new obligations to comply with - especially for processors and not only for controllers.
It is to be noted that the DPA 2017 does not specify the level of encryption that an organisation should provide. Depending on the category of personal data processed, it is the responsibility of the controller to choose the appropriate level.

However, the Data Protection Office recommends organisations to regularly assess whether their encryption method remains appropriate rather than developing a custom algorithm.

Anonymity:

Anonymity is fundamental for the full exercise of the right to freedom of expression. It is especially critical in repressive environments in which certain types of protected expression are outlawed, and lack of anonymity could lead to criminal charges or other consequences. The spread of the internet and new technologies have created new possibilities for communication and free expression and opinion, including enabling anonymity[1].

The ability to transact and communicate privately and anonymously online, through the use of encryption software and other tools, is a necessary requirement for the full realisation of the rights to freedom of expression and privacy, particularly when speech may be socially taboo or critical of those in positions of power[2].
Anonymisation is a technique applied to personal data in order to achieve irreversible de-identification. The DPA 2017 does not provide a specific section to regulate "anonymous information".

It is to be noted that DPA 2017 does not apply to anonymous information/data that is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

4. National legislative and regulatory frameworks concerning the collection, processing, retention or use of personal data by Governments and other actors, in particular business enterprises, related human rights protection gaps and ways to bridge those gaps.

The general principle is that the consent of an individual is required before sharing of personal data can be done and that individual must be informed of that at the time of collection of the personal data, according to section 23 of the Data Protection Act 2017 (DPA). Furthermore, section 28 of the DPA, namely "lawful processing", lays down the conditions for legal basis required for processing such as obtaining the consent of the data subject before any processing.

The principles of fair and transparent processing require businesses and governmental bodies to provide information about themselves, give details on the purposes of processing, explain data subjects (individuals) how their personal data will be processed (e.g. existence of automated decision-making including profiling), elucidate the

[1] Association for Progressive Communications (APC) 2015 : The right to freedom of expression and the use of encryption and anonymity in digital communications http://www.ohchr.org/Documents/Issues/Opinion/Communications/AssociationForProgressiveCommunication.pdf
[2] Encryption and Anonymity in Digital Communications ,Office of the High Commissioner for Human Rights ,Consultation on the Right to Freedom of Expression and the Use of Encryption and Anonymizing Tools Online http://www.ohchr.org/Documents/Issues/Opinion/Communications/FreedomHouse.pdf

consequences of such processing, and inform individuals on their rights (e.g. existence of the right to withdraw consent).

The principles relating to processing of personal data must be lawful, fair, transparent, adequate, relevant, accurate, kept for as long as required, and proportionate to the purposes for which it is being processed. Where the purpose for keeping personal data has lapsed, the organisation must destroy the data as soon as is reasonably practicable and notify any processor or service provider holding such data.

There is no retention of the personal data at the level of the internet service providers and no regulation is in place which talk about retaining personal data at the level of organizations.

5. Growing reliance on data-driven technology and biometric data:
    a. How can new technologies help promote and protect the right to privacy?
    b. What are the main challenges regarding the impact on the right to privacy and other human rights?
    c. What are the avenues for adequate protection of the right to privacy against threats created by those technologies? How can the international community, including the UN, address human rights challenges arising in the context of new and emerging digital technology?

(a) The same technology that permits the collection, sharing and analysis of huge amount of data also allows for the incorporation into information systems of features that protect information from abuse or misuse. Three technologies that hold great promise are as follows:

1. anonymization techniques that allow data to be usefully shared or searched without disclosing identity;
2. permissioning systems that build privacy rules and authorization standards into databases and search engines; and
3. immutable audit trails that will make it possible to identify misuse or inappropriate access to or disclosure of sensitive data.

(b) Technological innovations are having a transformational impact on the way business is conducted, and the way people interact among themselves, as well as with government, enterprises and other stakeholders. Increasingly, an ever-wider range of economic, political and social activities are moving online, and personal data are the fuel that drives much of the online activities. As the global economy shifts further into a connected information space, the relevance of data protection and the need for controlling privacy increase further. With rapid proliferation of social networking, cloud computing, internet of things, and big data, individuals want to feel confident that their privacy is strongly

protected. Creating trust online is thus a fundamental challenge to ensure that the opportunities emerging in the digital economy can be fully leveraged.

(c) To address the challenges, a major data protection legislative reform is required. The aim of the reform is to create a more rigorous and coherent data protection framework backed by strong enforcement that allows the digital economy to grow and puts individuals in control of their own data thereby providing greater legal and practical certainty for economic operators and public authorities.

6. Undue interferences with the right to privacy in the digital age that may have particular effects for women, as well as children and persons in vulnerable situations or marginalized groups, and approaches to protect those individuals.

The global concern is about the need to understand how to reduce the risk of harm that children and women are exposed to while as well maximizing the opportunities for learning, participation and creativity in the digital age. This is an even more critical issue in marginalised societies where those concerned have limited access to resources that would guard them against the dangers of privacy infringement that are inherent in the increasing use of Information Technologies in our daily lives and therefore making them exposed to abuses that would inevitably affect their well-being in the society.

An effective way to protect the concerned women, children and persons in vulnerable situations is through sensitisation in order to create awareness about the impeded dangers of the digital age and the means to protect their right to privacy which is a fundamental Human Right.

Another approach is to take into consideration the ways that people of different age groups and social categories interact in the digital age when online technologies, networks, services and policies are being developed in order to be able to provide adequate measures to counteract the dangers involved and to have means of tracking and condemning the culprits.