Privacy, Data Protection, Development and Humanitarian agencies

BY MRS DRUDEISHA MADHUB

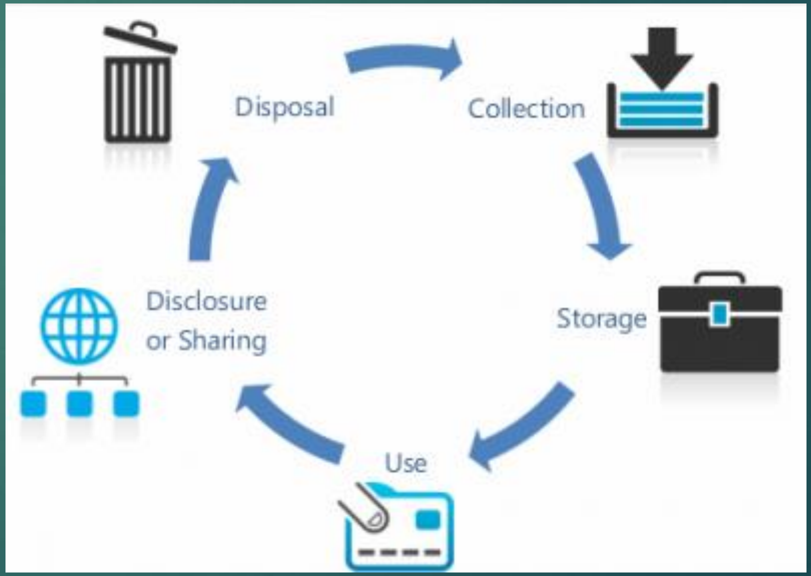
DATA PROTECTION COMMISSIONER (MAURITIUS)

Introduction

- The European Court of Human Rights has eschewed the definition of privacy, stating: “The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of ‘private life’.” An important issue for Internet privacy in general is the precise relationship between privacy and data protection or, to put it differently, the extent to which data protection principles find protection as part of the established human right to privacy. It is clear that the two issues are different and that data protection is not entirely subsumed into the concept of privacy. However, important data protection principles can be derived directly from the human right to privacy, and this finds support in international jurisprudence.

Introduction

- Data protection is the systematic application of a set of institutional, technical and physical safeguards that preserve the right to privacy with respect to the **collection**, **storage**, **use,** **disclosure** and **disposal** of personal data.
- Personal data includes all information that can be used to identify data subjects such as name, address, telephone numbers amongst others.



Humanitarian and other international organisations in the developing world

Collection of Personal data

- Humanitarian and development-oriented organisations collect a wealth of personal data from name and location to detailed medical information. Some of this data is collected without an assessment of whether it is really required to achieve the programme’s objectives or whether its collection might put beneficiaries at risk, now or in the future.
- In some situations, even collecting the most basic information is risky. For instance, the use of mobile phone networks to transmit information is a practice that is particularly problematic, as networks may be subject vulnerable to interference or state surveillance.

Issues

- Some humanitarian and development-oriented organisations may willingly pass beneficiary information on to donors or other third parties, such as commercial partners, <u>without a clear knowledge of what that information may be used for</u>.

- For example: A family receiving food aid might consent to giving information about their circumstances to an aid organisation, but not know that the data is later going to be used for commercial exploitation or other purposes.

- In passing on information to state actors, meanwhile, humanitarian and development-oriented organisations may unwittingly facilitate state surveillance, adding pieces to the jigsaw of information that allows a state to track and monitor an individual’s life.

Issues

- **Leaks of personal data have potential to result in individuals being targeted for violence or harassment**, due to ethnicity, religion, medical history, or just because they have received aid or worked with international organisations. This is a major concern for aid agencies, whose mandate is to uphold the humanitarian principle of ‘do no harm’. Risks to the protection of beneficiary data are faced at every stage.

Existing efforts to protect beneficiary information

- There are increasing efforts in the humanitarian and development-oriented communities to improve practices regarding beneficiary data protection.
  - The most developed standards come from the International Committee of the Red Cross whose *Professional standards for Protection Work* carried out by humanitarian and human rights actors in armed conflict and other situations of violence contain statements such as, "protection actors seeking information bear the responsibility to assess threats to the persons providing information, and to take necessary measures to avoid negative consequences for those from whom they are seeking information."
  - A recent report by the New America Foundation, *Dialing Down Risks: Mobile Privacy and Information Security in Global Development Projects* proposes principles for promoting privacy in the context of the use of mobile phones.

Existing efforts to protect beneficiary information

- A consortium of non-governmental organisations, led by the Cash Learning Partnership, is working to develop guidelines around protecting beneficiary data in e-transfer programmes.

- The UN Refugee Agency, UNHRC, and the World Food Programme are known to be developing internal guidance around beneficiary data protection.

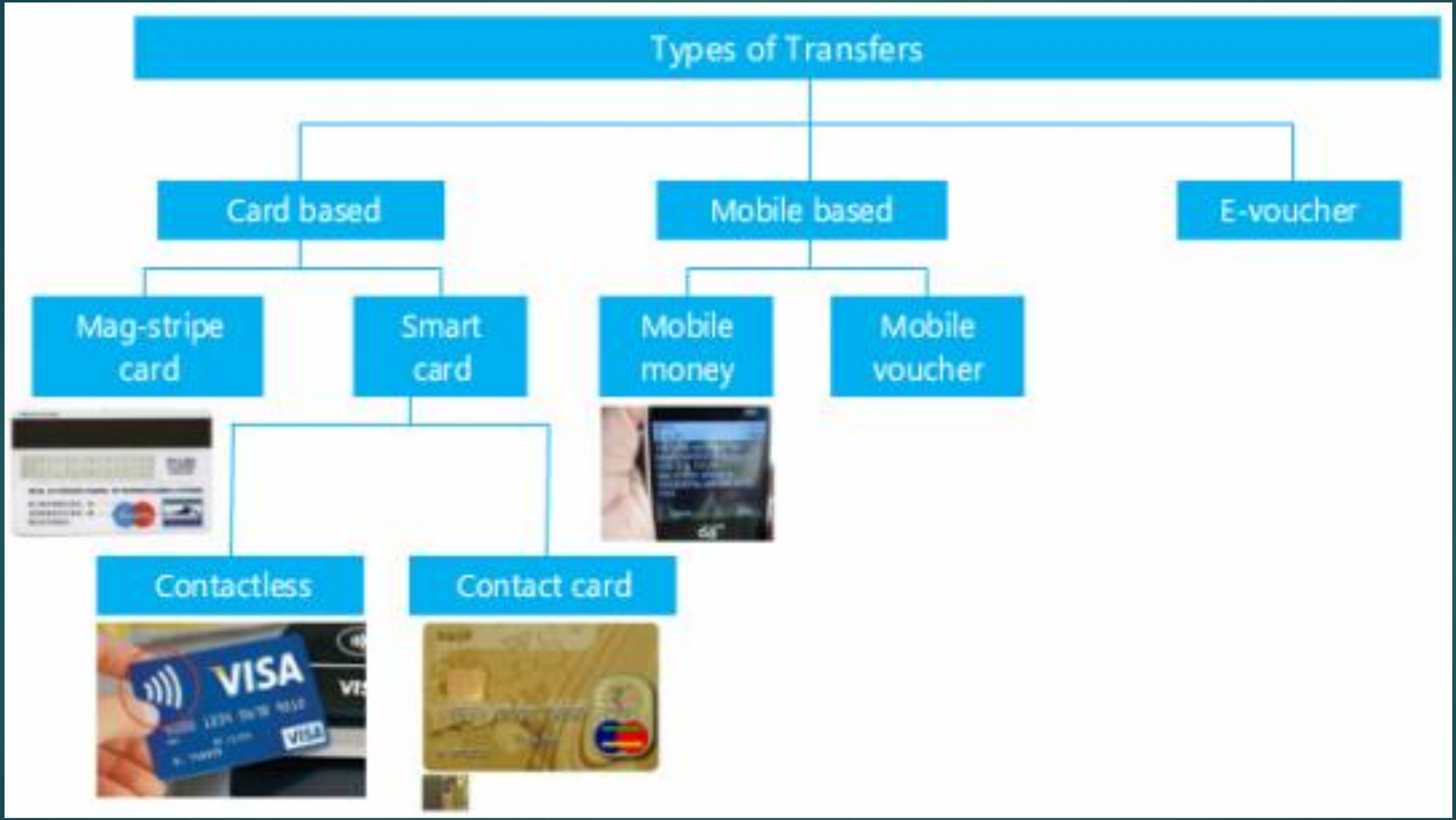
- There have also been industry-driven initiatives, such as the Guidelines for the Use of SMS in Natural Disasters, produced by the GSMA, an influential association of mobile operators. These guidelines recognise the importance of keeping text messages confidential and hosted on a secure platform, as well as the need to obtain consent before transferring personal data to third parties.

E-transfers and their associated risks

- Where feasible and appropriate to the context, e-transfer technology is increasingly being adopted by aid agencies, which can allow programmes to reach affected populations at a large scale and in hard-to-reach environments.

- It is the adoption of e-transfer technology, and digital technology more generally on programmes, that is driving an increasing realisation within the humanitarian sector of the **privacy risks** associated with the collection, use, storage, sharing and disposal of beneficiary data. A failure to understand or mitigate these new threats throughout the programme cycle can put people at risk and undermine the trust that humanitarian organisations require in order to do their work.

Types of Transfers



- E-transfer programmes begin with the **collection** of personal data from beneficiaries for example, on some e-transfer systems, client ID is verified using biometric data and this requires the collection of highly personal data from beneficiaries such as photos, finger prints and retina scans.
- Once collected this information is **stored** by the agency and will be **used** by the agency to prepare beneficiary lists. The data may be **shared** with partner agencies and wider stakeholders including for example, national governments administering social protection programmes , or potentially with donors who are funding the intervention. This raises a number of risk factors to be considered, for example:
  - ***Who within the agency is collecting this personal information?***
  - ***How is it being collected?***
  - ***How and where is this data being stored?***
  - ***Who has access to the data?***
  - ***How is it being shared with partners and other stakeholders? What is being shared? How are partners storing and using this data?***
  - ***How is all of this being communicated to beneficiaries and their consent obtained?***
  - ***How long will the data be kept for and what will happen to it afterwards?***
  - ***If the programme scales up – Can the data management system cope and maintain its integrity?***

Good Practice

- There are several good practice approaches agencies can put in place to overcome some of the challenges associated with protecting beneficiary data on e-transfer programmes.
- Many organisations are taking the following approach, that can be seen as emerging good practice in finding solutions pertinent to specific programme locations:
  - Getting a better understanding of the importance of ensuring beneficiary privacy and the implications of not doing so.
  - Understanding what constitutes their due diligence in this regard. What are the core principles that they should be adhering to? What is the overriding Government policy on data management?

Good Practice

- Either as part of preparedness measures or following response analysis, organisations are undertaking risk analysis to gain a better understanding of the data protection risks and related implications for the specific programme context. This includes considering: size and scale of the planned programme, beneficiary profile and vulnerabilities, location, duration, cash assistance amount, delivery mechanism and wider legislation (including: host country, donor country, third party policies).
- Considering their mandates and the contexts in which they operate, public and private sector organisations are applying these risk analysis techniques to the project and data management cycles, and developing organisationally relevant documents.

Digital identity registration and biometrics

- Technologies are changing the impact and importance of identity registration in two ways: first, they are enabling the digitisation and centralisation of personal information, its use across government services, and the continual checking of identity. Second, technological advancements have facilitated the capture, processing and retention of biometrics, physical traits of individuals including fingerprints, facial scans, iris scans, or even DNA.

- One of the predominant reasons why digital identification systems, particularly those containing biometrics, have faced resistance in developed countries is the potential for scope creep: once collected, biometrics can be re-used for a variety of other purposes. Therefore, a system that is designed for the purpose of disbursing aid and entitlement services will soon be used for verifying citizenship and age, and biometrics may be checked and compared with those for policing purposes.

Privacy Impact Assessment (PIA)

- Privacy is not a privilege – a comfort that desperate people should have to give up. It is a fundamental human right, enshrined in the United Nations Universal Declaration of Human Rights.

- Though some IGOs are exempt from these requirements, such organizations must strive to implement best practices with regard to privacy, ethics, and data protection.

- The first step is to carry out a Privacy Impact Assessment (PIA). A PIA is a tool used to identify, analyse, and mitigate privacy risks arising from technological systems or processes.

- The PIA help organisations to:
  - consider the types of personal data they are processing;
  - reduce the risk of harm to individuals through the misuse of their personal information;
  - design more efficient and effective processes for handling personal data; and
  - question whether it is necessary to process personal data to provide a service or deliver a project.

RECOMMENDATIONS:-

- Constitutional measures
  - Strong constitutional protection should be provided for both privacy and freedom of expression. This should encompass positive protections for these rights and, ideally, impose a positive obligation on the State to provide protection against private interferences with these rights.
- CIVIL AND CRIMINAL SANCTIONS
- CORPORATE POLICIES
  - A possible set of principles to underpin a corporate policy on privacy could be as follows:
  - (1) No Surprises. Companies and services should only use, collect and share information about users as disclosed in clear, concise, easy to understand, notices.
  - (2) Real Choices. Companies and services should give users actionable and informed choices by providing clear information at the point of collection and providing a choice to opt-out whenever possible.

RECOMMENDATIONS:-

- (3) Sensible Settings. Companies and services should establish default settings in products and services that balance privacy, security and user experience.
- (4) Limited Data. Companies and services should collect and retain the least amount of information necessary for the feature or task and meet users' reasonable expectations of privacy. Anonymous, aggregate data should be used whenever possible, and personal information collected should only be kept for as long as necessary to serve the purpose it was collected for.
- (5) User Control. Companies and services should not track or disclose personal user information without the user's consent. They should employ privacy enhancement that put people in control over their information and enable them to understand how their information is being used and stop collection and tracking of their personal information if they choose.
- (6) User Access. Users should have the right to know when their data is being collected or processed and to access that data in an understandable form. This information should be provided to users without charge and they should have the power to delete or correct errors in information.

RECOMMENDATIONS:-

- (7) Trusted Third Parties. Companies and services should make privacy a key factor in selecting and interacting with partners. In addition, all third party companies, services, and applications should uphold these privacy principles.
- (8) Security. Companies and services should take appropriate measures to protect data against both natural and human risks, including unauthorized access, misuse or error. If a website or service's security is breached, users have a right to know immediately.
- (9) Transparency of Government Sharing. Companies and services should notify users about government requests for information associated with users' accounts when permitted to do so by law, giving users the opportunity to contest that demand for their data if they choose to.
- (10) Providing Remedies: Where a company identifies that they have caused or contributed to adverse impacts on users' privacy, they should make provision for, or cooperate in, handling complaints and providing a remedy to those users through a transparent process.
- (11) Privacy Across the Board. Privacy protections should apply equally across all online and mobile platforms and to all companies, services and third-party applications. Companies should also make sure partners uphold strong privacy principles

Conclusion

- While technologies and new programmes may help target, support, and secure development, their adoption must be subjected to rights-based questions about whether they are the necessary, proportionate, and effective methods for development, and whether legal frameworks exist to protect against privacy abuses.
- The challenge is to improve access to and understanding of technologies, ensure that policy makers and the laws they adopt respond to the challenges and potentialities of technology, and generate greater public debate to ensure that rights and freedoms are negotiated at a societal level.

References

- https://www.privacyinternational.org/node/391