Legal Aspects of Internet Governance

Peter Major
Vice-chair, UN Commission on Science and Technology for Development

Outline

- Legal frameworks and the Internet
- Legal issues and the Internet Governance
- Privacy and data protection
- Personal Data
- Data Protection Principles
- General Data Protection Regulation (GDPR)
- Conclusion

Legal frameworks and the Internet

- Global frameworks
  (treaties, conventions, covenants, regulations, guidelines, etc.) - no global treaty on Internet
  e.g.: UN Charter, CRPD, Radio Regulations, ITRs, etc.
- Regional frameworks
  e.g.: CoE Budapest Convention on Cyber Crime, EU GDPR, etc. - direct and indirect reference to the Internet
- National frameworks

Human Rights Council – rights off-line apply on-line

Legal issues and the Internet Governance

- Human rights
- Critical resources
- Privacy and data protection
- Consumer protection
- IP rights, trade mark protection, gTLD dispute, geo name protection, etc.
- Net neutrality

Privacy and Date Protection

- Privacy - freedom from observation, intrusion, or attention of others
- Privacy rights are not absolute
- Balance needed
  - Individual rights
  - Society's needs (sometimes trump individual privacy)
- Privacy and "due process"
- Privacy is a function of culture, means different things in different countries and regions
- Data protection - the process of safeguarding important information from corruption, compromise or loss

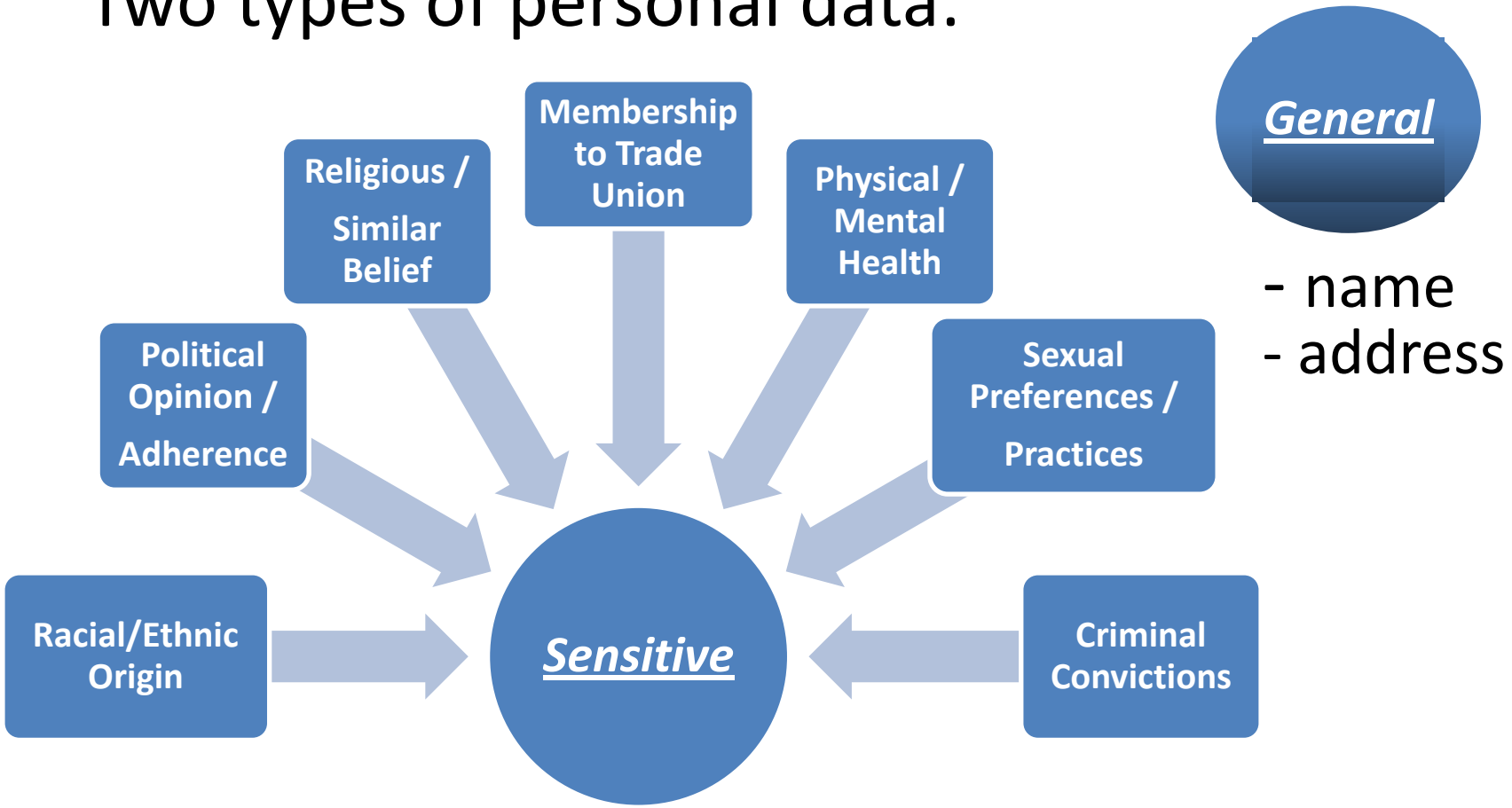
Personal Data - Definition

- Data which relate to an individual who can be identified from those data

- Can be on paper, on an IT system, on a CCTV system, etc.

Personal Data - Types

Two types of personal data:



Personal Data - Terms

Data Controller:

An individual or an organization (either public or private), who decides as to how personal data is to be collected and used

Data Processor:

Organizations which process personal data for and on behalf of another organization (data controller)

Personal Data - Processing

Any operation or set of operations performed on the data wholly or partly by automatic means, or otherwise than by automatic means, and includes

- collecting, organizing or altering the data;
- retrieving, consulting, using, storing or adapting the data;
- disclosing the data by transmitting, disseminating or otherwise making it available;
- aligning, combining, blocking, erasing or destroying the data;

Data Protection Principles

1. Personal data shall be processed fairly and lawfully

2. Personal data shall be obtained only
   - for any specified and lawful purpose,
   - and shall not be further processed in any manner incompatible with that purpose

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are processed

Data Protection Principles (cont'd)

4. Personal data shall be accurate and, where necessary, kept up to date

5. Personal data processed for any purpose shall not be kept longer than is necessary for that purpose(s)

6. Personal data shall be processed in accordance with the rights of the data subjects

Data Protection Principles (cont'd)

7. Personal data shall not be transferred to another country, unless that country ensures an adequate level of protection for the rights of data subjects in relation to the processing of personal data

8. Appropriate security and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

General Data Protection Regulation

- The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area.

- The protection of natural persons in relation to the processing of personal data is a fundamental right

- GDPR protects the personal identifiable information of individuals with permanent residence in the EU

General Data Protection Regulation (cont'd)

- Any company that controls personal data or processes personal data, by itself or on behalf of another company, must comply with the GDPR, even if the company is based outside the EU
- Explicit and retractable consent must be provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.
- Right to access and portability - Data subjects can request confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format.

General Data Protection Regulation (cont'd)

- Privacy By Design - legal requirement for the inclusion of data protection from the onset of the designing of systems, rather than a retrospective addition.

- GDPR also significantly increases the possibility of higher fines and sanctions to non-compliant companies: up to 20 million euros or 4% of annual turnover

- Came into force as of 25 May 2018

Scope of the GDPR

- GDPR applies to all
- GDPR widens the definition of personal data e.g.: genetic, mental, cultural, economic or social information
- GDPR tightens the rules for obtaining valid consent to using personal information

Effects of the GDPR

- GDPR makes the appointment of a data protection officer (DPO) mandatory for certain organizations: in Europe in the next two years appointment of 28000 DPOs is estimated

- GDPR introduces mandatory privacy impact assessments (PIAs) to
  - Ensure conformance with applicable legal, regulatory, and policy requirements for privacy;
  - Determine the risks and effects; and
  - Evaluate protections and alternative processes to mitigate potential privacy risks.

Effects of the GDPR (cont'd)

- GDPR introduces the right to be forgotten
- GDPR introduces a common data breach notification requirement: within 72 hours after discovering it
- GDPR expands liability beyond data controllers
- GDPR requires privacy by design
- GDPR introduces the concept of a one-stop shop (central point of enforcement)

GDPR Compliance

- Ensure key departments are aware that the law is changing, and anticipate the impact of GDPR.
- Document what personal data is held, where it came from and with whom it is shared.
- Review current privacy notices, and make any necessary changes.
- Review procedures to address the new rights that individuals will have.
- Plan how to handle requests within the new time frames, and provide the required information.

GDPR Compliance (cont'd)

- Identify and document the legal basis for each type of data processing activity.
- Review how consent is sought, obtained
- and recorded.
- Make sure procedures are in place to detect, report and investigate data breaches.
- Designate a Data Protection Officer to take
- responsibility for data protection compliance

Conclusion

- GDPR - regional framework with effects beyond EU
- GDPR – an example of the need to review applicability of legal frameworks to cyber space:
  - analyze of existing framework
  - identify missing elements if any
  - modify framework if needed
  - allow time before introducing new framework
- Inherent contradiction – rapidity of changes in technology & relatively slow policy development process - 20 years to replace EU directives

Glossary

- ECOSOC – UN Economic and Social Council
- ICANN – Internet Corporation of Assigned Names and Numbers
- ILO – International Labour Organization
- IEEE – Institute of Electrical and Electronics Engineers
- IETF – Internet Engineering Task Force
- ISOC – Internet Society
- ITU – International Telecommunication Union
- UN – United Nations

Glossary (cont'd)

- UNCTAD – UN Conference on Trade & Development
- UNDP – UN Development Projects
- UNESCO – UN Educational, Scientific and Cultural Organization
- UNGA – UN General Assembly
- W3C – World Wide Web Consortium
- WHO – World Health Organization
- WIPO – World Intellectual Property Organization
- WTO – World Trade Organization

Global Frameworks

- UN Charter
- Universal Declaration of Human Rights
- International Covenant on Civil and Political Rights
- International Covenant on Economic, Social and Cultural Rights
- Convention on the Elimination of All Forms of Discrimination Against Women

Global Frameworks (cont'd)

- Convention on the Rights of the Child
- Convention on Rights of Persons with Disabilities
- ITU Radio Regulations
- ITU International Telecommunication Regulations (1988)
- ITU ITRs (2012)
- WIPO Copyright Treaty

Global Frameworks (cont'd)

- WIPO Performances and Phonogram Treaty
- WIPO Geographical Indications
- WIPO Global Brand Database
- WTO Trade –Related Aspects of Intellectual Property Rights TRIPS
- ISO-3166-Countries-with-Regional-Codes
- WIPO Uniform Domain Name Dispute Resolution Process (UDRP)
- ICANN Rules for UDRP

Regional Frameworks

- EU General Data Protection Regulation - GDPR
- Council of Europe Convention on Cybercrime

Guidelines, Principles Recommendations

- United Nations Guidelines for Consumer Protection - UNCTAD
- OECD Recommendations on Consumer Protection in E-commerce
- Consumer Policy Guidance on Mobile and Online Payments
- OECD Identity theft
- Manila principles on Intermediary liability
- EU rules on net neutrality