Data Protection & Privacy

Professor Ian Walden
Institute for Computer and Communications Law
Centre for Commercial Law Studies, Queen Mary, University of London

Introductory Remarks

- Technology and Personal Data
  - Immense power to process and store data
- Information Economy
  - Data: Driver of economic growth
- Consumer Privacy Concerns
  - Barrier to consumer e-commerce….

…An Irreconcilable Paradox?

Privacy & Data Protection Laws

- Privacy laws
  - Universal Declaration of Human Rights (1948), art. 12
    - 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'
- Data protection laws
  - e.g. EU Directive 95/46/EC
    - (a) Personal data, (b) Justified processing, (c) Right of access and (d) Independent authority
  - Bahamas (2003), Costa Rica (2011), Saint Lucia (2011), Trinidad & Tobago (2011) and Antigua (2013)

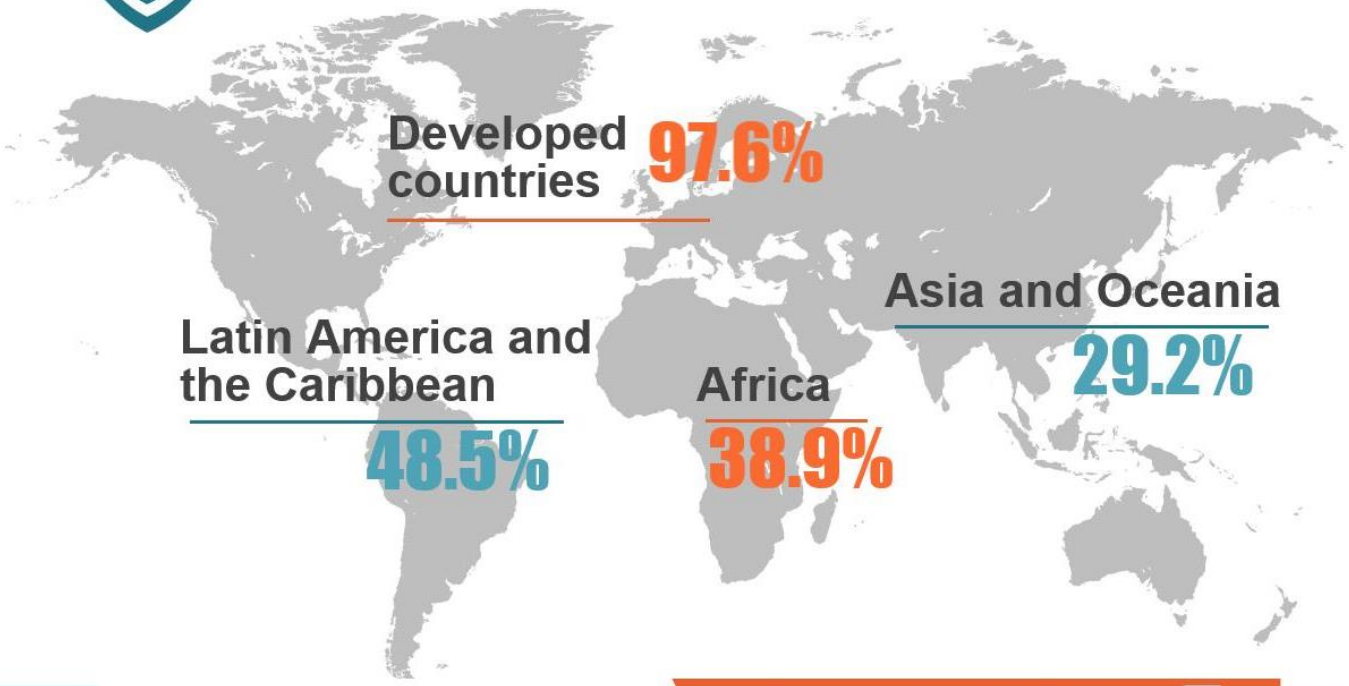
UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT

UNCTAD

PROSPERITY FOR ALL

Cyberlaws and regulations for enhancing e-commerce around the world 2014

Share of countries with privacy and data protection laws



Source UNCTAD, 2015

Information Economy Report #IER2015

International developments

- There is life beyond the EU.....
  - Over 100 jurisdictions have laws
    - Not including constitutional provisions
- A spectrum of measures
  - From binding instruments to self-regulation
  - Regional and international
- Motivations
  - Privacy (internal) & trade (external) concerns
  - Customer-led pressure
    - ‘Ad-blocking’ wars

International initiatives

- Council of Europe Convention (1981)
  - Amended 2001
  - Modernization process
- OECD Guidelines (1980)
  - Revised (2013)
- United Nations Guidelines (1990)
- Commonwealth Model Privacy Act (2002)
- APEC Privacy Framework (2004)
  - Cross-border privacy enforcement arrangement
- ISO/IEC 29100: 2011 Privacy framework

Categories of Personal Data

- Personal data
  - “any data concerning an individual from which that individual is directly identified or indirectly identifiable”
- Sensitive Data
  - Information likely to embarrass or cause discrimination needing enhanced protection
- Consensual & non-consensual data
  - Data provided with or without knowledge and consent

Sensitive Data

- EU Directive 95/46/EC
  - Health and Medical Data, Race/ethnicity, Gender, Union/trade membership, Religious or philosophical belief, Sexual orientation, practices, Political affiliation, Criminal history
    - Telecoms sector: traffic data & location data
    - Reform proposals: genetic data & biometrics
- Trinidad & Tobago
  - ‘personal data’ Marital status, education or employment history, financial transactions, fingerprints….
    - And ‘sensitive personal data’

Imposing obligations

- Data controllers
  - Data processors
    - Processing ‘on behalf’ of a data controller: knowledge?
    - Contractual requirements & regulatory obligations
    - Joint and severable liability
- Processing principles
  - Interests relating to data subjects
    - Transparency, access & objection
  - Interests relating to data quality
    - Accuracy, adequacy, complete, up-to-date, secure

Applicable law

- Public & private sector?
  - e.g. Trinidad & Tobago
- Territorial scope
  - Directive 95/46/EC
    - Establishment or equipment
    - Reform: Processing related to the offering goods or services to Union data subjects (targeting) or monitoring behaviour
- Foreign laws
  - Legal obligations & public interest processing
    - EU or national law *not* USA Patriot Act

Fair Processing Principles

- Collection
- Proportionality
- Use
- Data Quality
- Transparency
- Access and Correction
- Objection
- Transfers
- Security
- Accountability

Collection

- Data to be fairly and lawfully obtained
- Data subject consent: consensual data
  - freely given, specific, informed
  - Explicit or implicit: ‘opt-in’ or ‘opt-out’
- Necessary for specified reasons: non-consensual
  - Legal requirements: e.g. EU Directive 06/24/EC on data retention – declared invalid!
- Ability to exclude data from certain processing
- Consequences for failure to provide data

Proportionality

- Personal data should be adequate, relevant and not excessive to the purpose for which it is collected

Use Limitation

- No disclosure, transfer or other use except those needed to achieve the purposes specified except:
  - With consent of data subject
  - Pursuant to law
    - e.g. employer tax reporting

Data Quality

- As needed for specified purposes, collected and stored data should be
  - Accurate
  - Complete
  - Up to Date

Transparency

- Data subjects should have the means to know:
  - Of the existence and nature of processing
  - The nature of the personal data collected and used
  - The purposes of their use
  - The identity and location of the entity controlling the processing
  - Whether any data is likely to be transferred and to whom

Access and Correction

- Right to have controller confirm processing
  - Public register
- Right to a copy of the data held
  - Reasonable timeframe and cost
  - Intelligible format
- Right to correct inaccurate/incomplete data
  - Google & the ‘Right to be forgotten’
- Right of ‘data portability’?
  - Social media

Objection

- Individuals should be able to object to certain processing of their data
  - e.g. Marketing Purposes

Transfer

- Personal Data should not be transferred to third parties not providing the same level of protection
  - International data flows

Security

- Appropriate measures by data controller to guard against:
  - Loss or destruction of data
  - Unauthorised processing or disclosure
- “Appropriate” to risk presented
  - Nature of data
  - Nature of processing
- Technological, organisational measures
  - Security breach notification obligation

Accountability

- Redress for unlawful processing
  - Damages, injunction
    - Economic & distress
  - Criminal & administrative sanctions
    - e.g. 5% of global turnover!
- System of enforcement
  - Controller's compliance to be subject to oversight
    - Regulatory agency, Commissioner
    - Private compliance schemes
      - e.g. Truste (and the FTC)

Regulatory models

- Omnibus data protection regulation
  - e.g. the European Union
- Sectoral Regulation
  - e.g. the United States
    - Federal government, health, finance, children, video recordings
  - e.g. Europe
    - Directive 02/58/EC ‘privacy and electronic communications’
- Self / Co-Regulation
  - e.g. Australia
  - Codes of conduct, e.g. T&T

Regulatory oversight

- Public authorities with ‘complete independence’
  - Funding issues
  - Regulatory costs, e.g. EU €2.3bn per year (€130m on notifications)
- Supervision & enforcement
  - As surrogate for data subjects: ‘independent guardian’
    - ‘associations representing data subject interests’
  - More effective deterrent
- Internalising compliance
  - In-house (independent) data protection officers
  - Privacy impact assessments

Regulating Transborder Data Flows

- Protecting data subjects
  - 'adequate level of protection'
- Exceptions
  - Consent, contractual performance
  - Legal obligations (whose)?
- Non-tariff trade barrier?
  - WTO GATs, Article XIV: *General Exceptions*

    '(c)(ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;'

Approaches to Adequate Protection

- 'in all the circumstances'
  - e.g. security, duration
- Contractual obligations achieving adequacy
  - Individual & EU model contract terms
    - Controller-controller, controller-processor, processor-sub-processor
  - Binding corporate rules for intra-company transfers
- Mutual recognition
  - Commission Decisions
    - e.g. Argentina (2003), Canada (2002), New Zealand (2013) and Eastern Republic of Uruguay (2012)
    - US 'Safe Harbor' Arrangement (2000)
      - AG Opinion in *Schrems v Data Protection Commissioner* (23 September 2015)

Concluding Remarks