Digital Identity: Principles on Collection and Use of Information

UNCITRAL Colloquium on Legal Issues Related to Identity Management and Trust Services
21-22 April 2016

Anurag Bana
Legal Policy & Research Unit
International Bar Association
Background

Digital tsunami of personal data
- Broader set of digital information
- Opting out not a realistic option
- Global phenomenon

Inadequate legal definitions & attendant protections
- Extent of collection & use not readily ascertainable
- Multiple players claim/expect various types of rights

User not fully in control of information
- Do not cover full scope of digital identity /PII
- Efforts to bridge the gaps are jurisdictionally bound
- Harmonized approach needed for this global issue
IBA Working Group’s Mandate

Overarching aim – To provide for transparency, responsibility and security, with the underlying premise that users should have control over their identifiable information.

Ultimate objective – To arrive at a set of Principles that would be agreed to and adopted by all stakeholders, following consultation and input.

To develop a set of High-Level Principles around the collection, use and sharing of digital identity information.
Considerations Underpinning the Principles:

- Roman law distinction between rights ‘in rem’ and rights ‘in personam’
- ‘Right to erasure’ under EU’s General Data Protection Regulation Article 17
- “California Right to Know Act”
- The United States Freedom of Information Act (FOIA)

- Possibility of fraud can never be eliminated- acceptance of the “Neighbour Principle”.
- Tension between increasing online security access and ease of communication

**Rights Over Data**
(PI ownership to the persons to whom that information relates)

**Protection of Data**
(Need to secure reliability and authenticity of digital information.)

**Effective Remedies**
(Actionable either before the NEB or before the courts)

**Enforcement Mechanisms**
(Quick; Effective; Consumer friendly; Low cost; Global in application)

Include -
- i) the possibility of an immediate action or intervention to end a factual threat or hazard under appropriate mechanisms of coercion
- ii) the proper repair of harm done, either in pecuniam or in kind.

**Internet Corporation for Assigned Names and Numbers (ICANN) model used to ensure each jurisdiction has a National Enforcement Body (NEB).**
The collective aspect of the set of characteristics by which a thing is definitively recognisable or known.

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

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

Information, such as an identification number, used to establish or prove a person’s individuality.
Principle 1: Transparency

Data collectors should maintain transparency, and inform users of:

a. What data is being collected and purpose?;
b. How the data will be used?;
c. Who will it be shared with?;
d. How long the data will be retained?; and

e. Method of data storage.

This Principle requires that “terms of use” and “privacy polices” are clear, concise and accessible to online users.
Principle 2: Responsibility

Collector
- provide user controls.
- notify users of changes to any privacy settings or terms of use

User
- able to choose from privacy settings e.g. opt ins and opt outs
- able to correct any inaccuracies on the online database that relates to their PII.
- able to request the destruction of user identifiable information in some limited circumstances.

Privacy settings easy to implement.
Google (Case Study)

- ECJ “Right to be Forgotten” case.¹

- A Dutch Court confirmed that the “right to be forgotten” is not an absolute right, it has to be balanced against the right and interests of intermediaries.²

---

¹ Case C-131/12 Google Spain SL, Google Inc v Agencia Espanola de Proteccion de Datos (AEPD), Mario Casteja Gonzalez
² Court of First Instance of Amsterdam, 19 September 2014 (Summary Injunction)
Google Case in Israel – Attorney Defamation

• An Israeli attorney was mischaracterized as having committed five acts of unethical attorney behaviour when in fact he only represented the Israel Bar Association in disciplinary proceedings related to the liable attorney.

• Google's search algorithm made it appear as if he was the attorney who was convicted.

• The court reversed a magistrate’s preliminary opinion and asked Google to remove search results that were clearly defamatory in nature.  

3. District Court of Tel-Aviv, 49918-05-12, Amir Savir v. Google, July 5, 2015
Principle 3: **Security**

Collectors should implement adequate safeguards to:

- Protect the security of the user information/data
- The protection should be commensurate with how sensitive the user information/data is.

**Consequences of failing to protect online data**

- Financial loss to businesses
- Reputational damages to the firm (e.g. data collector)
- Damage to the industry, economic infrastructure and or threat to national security
- Possible questions of professional misconduct
Security (Cont.)

• In a recent study, law firms citing information security as their top concern doubled from 23% in 2012 to 46% in 2014.4

• A report released in May 2015 (Juniper Research) predicts that the global cost of data breaches will reach $2.1tn in 2019.5

• 2013 survey – 80% of partners and IT directors in law firms believed they were likely to be subject to a cyber-attack.6

• In response to the Question: ‘For which of the following do you believe your general counsel/legal department would benefit from additional expertise?’ – 67% of respondents named ‘cyber security risk’ as one of their choices.7

---

6. Anna Reynolds, ‘Fears of Cyber Crime Rise As Nearly 80% Believe Their Firm Could Be Hit By Web Hack’ (Legal Week, 3 May 2013)
Apple Inc (Case Study)

- In response to recent theft of photos from digital online iCloud accounts:

Apple has announced that it has expanded its use of “two-step verification” to protect data stored online by its customers.  

Sustainable Development Goal (SDG) 16 and Cyber Security

**SDG 16.3** – *Promote the rule of law at the national and international levels and ensure equal access to justice for all.*

- Professional services store confidential client information on digital platforms which has the risk of being lost or stolen.

- To discharge their ethical obligations, lawyers must implement adequate cyber security measures to protect client information online and promote the rule of law in line with the spirit of SDG 16.

- Find the right balance between Security, Cost and Usability depending on the type of application.
Annex
Actors Who Claim Right to Data

Many players beyond users claim rights to use personal and professional data, these include:

- Platform or service providers
- Mobile application providers
- Data brokers
- Third parties interacting with the users.
Social Media Platform Providers

(Case Study)

Study conducted by IBA Legal Policy & Research Unit on six major social media platforms

1. Facebook
2. Google+
3. Twitter
4. LinkedIn
5. Tuenti
6. WhatsApp

Terms of use easy to find in all the identified platform providers.

Most platforms providers had instructions about the use of information that they collected, except Tuenti.

All platform providers collect personal information whenever the user accesses the service.

Movement of user information is controlled by the collector.

All users on the various platforms had the right to access, amend or remove information.

Most of the platform providers have the right to pass information on to others.
“Privacy Policies” and “Terms of Use”

• Online data collectors rely on “privacy policies” and “terms of use” as the basis for contractually accessing personal and professional user information.

• However, the terms are often unclear, and opting out settings on online platforms are difficult and ambiguous.
Facebook (Case Study)

• Facebook’s data scientists manipulated news feeds to perform a psychology experiment on over 600,000 users.²

• Question: *should users have expected this type of research when they agreed to Facebook’s “terms of use”?*
German Court Rules Against Use of Facebook "like" Button

• The Dusseldorf District Court ruled against an online shopping site's use of Facebook's "like" button.

• The court said that retailer Peek & Cloppenburg failed to obtain proper consent before transmitting its users' computer identities to Facebook, violating Germany's data protection law and giving the retailer an undue commercial advantage.3

• Peek & Cloppenburg potentially may face a penalty of up to 250,000 euros ($275,400) or six months' detention for a manager.

3. Victoria Woollaston, ‘Court Rules Against the Use of Facebook's Like button: Shopping Site Accused of Violating German Privacy Laws’ (Daily Mail, 9 March 2016)
Digital identity: principles on collection and use of information
Draft – April 2016

Other Ongoing IBA Research Work

- Disruptive Innovation and the Legal Profession.

- The Impact of Blockchain Technology in the Legal Services Industry and in the Legal Profession.
For further information, please contact:

**Anurag Bana**  
Senior Legal Advisor  
Legal Policy & Research Unit  
International Bar Association  
[anurag.bana@int-bar.org](mailto:anurag.bana@int-bar.org)  
Tel: +44 (0)20 7842 0090  
Web: [www.ibanet.org](http://www.ibanet.org)