Big Data Meets Regulation:
Global Trends in Data Protection Regulation and the Governance of Privacy

Image: © Shutterstock: jijomathaidesigners

Dr Katharine Kemp
Research Fellow
Digital Financial Services Research Team
Faculty of Law, UNSW Sydney
k.kemp@unsw.edu.au

“We don’t need you to type at all. We know where you are. We know where you’ve been. We can more or less know what you’re thinking about.”

Eric Schmidt, CEO, Google, 2010.

Outline

1. What are the potential **benefits** and **harms** from data-driven innovations and big data analytics in financial services?
2. What are the **origins** and **criticisms** of the informed consent (or notice and choice) approach to data protection regulation?
3. How is the **EU GDPR** affecting global trends in the governance of data privacy and what is its response to the criticisms of consent?
4. How do the recent decision of the **Supreme Court of India in *Puttaswamy*** and related developments in India compare?

Benefits and Harms from Data-Driven Innovations and Big Data Analytics

UNSW SYDNEY

Benefits

- **Tailoring** new products to customer needs based on their behaviour and demographic information
- Assessing **creditworthiness** for “thin file” or “no file” consumers, those without a formal credit history
- Beneficial **competition** from new players, including mobile network operators, online platforms, social media – **data and networks**
- **Identifying** customers without formal ID documents
- **Verifying** the existence and scale of small businesses to provide credit

Potential harms – individual level

- Increased risk of **theft & fraudulent** use of personal information (incl biometric)
- Unanticipated **aggregation** of person's data from multiple sources to draw conclusions which may adversely affect **future credit, insurance or employment** or manipulate behaviour
- Disclosure of personal and sensitive information (eg, geolocation or political affiliation) to **governments** without transparent process and/or regard to the rule of law
- Decisions based on **inaccurate, unfair or unknowable conclusions** from data analyses (black box)
- Financial **exclusion** due to new data practices – market "segmentation" or "customization" which unfairly discriminates

Potential harms – social level

- Can work against important social benefits – eg **risk-pooling** via insurance
- **Constant surveillance** alone (the panopticon) is known to reduce the ability of humans to engage in independent, creative and innovative thought
- Pervasive **segmentation and differential treatment** of communities through the application of data analytics may threaten democratic values
- Inferences made about entire groups of people and interventions based on those inferences (**group privacy**)

Origins and Criticisms of the Consent Model

UNSW SYDNEY

Origins of “Informed Consent” or “Notice and Choice” Model

- US Fair Information Practice Principles (FIPPs) – 1970s – founded on “notice” and “choice”
- “Privacy control” or “privacy self-management”
- Customer has freedom and control to disclose and be “paid” for disclosures – leading to competition

Criticisms of consent model

- Do not read these notices
- Could not read these notices given the time it would take to read all (McDonald and Cranor – would take 244 hrs/yr, 6 working weeks, would cost US economy $781bn/yr)
- Could not understand the proposed uses if they did read them, let alone the consequences, especially given increasingly permanent data storage and complex and changing data uses and analyses
- Nor could they compare what the different providers offered and which protected their data more
- No ability to bargain with the firm for greater protection – take it or leave it

Effect of the Consent Model on Consumer Attitudes

Consumer trust and consent

"Qualitative Public Opinion Research with Canadians on Consent"
(Office of the Privacy Commissioner (Canada), March 2017)

- Want companies to highlight what personal information is collected; how it will be used and shared; how long it will be kept; and how it will be protected
- **Do not read** privacy policies because they are **long, complicated** and written in a language they **do not understand**
- Most **think they have little or no control** over when their information is used by a company
- Most **would like govt to make some rules** about how data can be used

Australian Community Attitudes to Privacy Survey 2017

Security concerns mean

93%

don't want their data to be sent overseas

79%

don't want their data shared with other organisations

58%

decided not to deal with some businesses

44%

avoid downloading smartphone apps

UNSW SYDNEY

Consent under the Privacy Act and the GDPR

EU GDPR

The **General Data Protection Regulation** 2016/679 was adopted by the European Parliament in April 2016, but will only begin to apply to EU Member States from **May 2018**.

The GDPR is intended to create certainty for business and enhance consumer trust, placing **additional obligations** on entities processing data in the EU.

Transfers of EU Data to Third Countries

Data can only be **transferred outside the EEA** if it is transferred:

- to an adequate jurisdiction (does not include Australia);
- to the US pursuant to the Privacy Shield;
- pursuant to another appropriate safeguard (eg BCRs, Model Clauses); or
- pursuant to a derogation (eg litigation; explicit consent).

When will the GDPR apply to us?

The **territorial scope** of the GDPR is broad, extending to controllers and processors not established in the EU if they process data which relates to data subjects in the EU.

Australian organisations will be affected by the GDPR if they:

- Are established within the EU;
- Offer goods or services to individuals in the EU; or
- Monitor the behaviour of individuals in the EU (likely includes tracking or profiling).

Some additional obligations under the GDPR

- Right to erasure of data (“right to be forgotten”)
- Right to object to processing (including direct marketing / profiling)
- Right to data portability
- Updated definition of acceptable “consent” by the data subject
- Fines up to 20 million euro, or 4 percent of annual worldwide turnover

Consent under Australian Privacy Act

In Australia, “consent” means “**express consent or implied consent**”. The four key elements of consent are:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific
- the individual has capacity to understand and communicate consent.

Consent under the GDPR

“Consent” now means:

> "any **freely given**, **specific**, **informed** and **unambiguous** indication of his or her wishes by which the data subject, either by a **statement or by a clear affirmative action**, signifies agreement to personal data relating to them being processed”

Consent under the GDPR

- Different types of uses require separate consent.
- “Bundling” multiple requests for consent may not be permitted.
- Implied consent or requiring consumers to “opt out” is insufficient.
- Silence, pre-ticked boxes or inactivity are not consent.
- Must have the right to refuse or withdraw consent at any time.
- Must be as easy to withdraw consent as to give it.

Justice K S Puttaswamy v Union of India (2017)

Puttaswamy outcomes

- **Privacy is a fundamental right** under the Constitution of India.
- Although privacy is not mentioned in the Constitution, the right emerges primarily from the guarantee of life & personal liberty.
- Privacy is the constitutional **core of human dignity**.
- But, like other fundamental freedoms, privacy is **not an absolute right**. Its invasion can be justified on the basis of a law which advances a legitimate state aim, which is proportional to its object.

Puttaswamy outcomes

"The Attorney General argued before us that the right to privacy must be forsaken in the interest of welfare entitlements by the State. … The **refrain that the poor need no civil and political rights** and are concerned only with economic well-being has been utilised through history to wreak the most egregious violations of human rights. … The **pursuit of happiness is founded upon autonomy and dignity**. Both are essential attributes of privacy which makes no distinction between the birth marks of individuals."

Current developments in India

- **Over 1 billion** people in India have been issued with an **Aadhaar** number linked to their biometric data – iris scans and fingerprints.
- Reports of Aadhaar **data leaks** and fraud and people being refused social welfare payments due to mismatches with their biometric data.
- From July 2017, the Indian government constituted a committee to make a proposal for a **data protection bill**.
- In July 2017, the **Reserve Bank of India** published **The Indian Household Finance Report**, which proposes an alternative model for data protection regulation.

RBI Indian Household Finance Report

- A **consent-based model for data protection is no longer appropriate**, given the implausibility of consent, especially in light of big data and machine learning. Propose instead a **rights-based model**.
- Consent would no longer be required for collection but would have a right to:
  - Fair treatment
  - Information
  - Data Security
  - Against Processing

Data Collection – Not a "Use-Based System"

- It is not sufficient to regulate only the use of data.
- The **mere collection of data creates serious and cumulative risks** – especially since data collected now is likely to exist forever, and grow as it is aggregated with other data; **growing risk it will be hacked**.
- A use-based system does not address harms to society from **pervasive surveillance**.
- A key focus of regulation should be to minimize the collection and storage of data.