Insurance regulators’ role in consumer data risk protection

Stefanie Zinsmeyer | May 2018 | Accra
Technology has allowed businesses to **better understand** and **serve consumers** through the collection and analysis of big data.
Data types being used in emerging markets

Source: Nordin et al., 2018
But how to balance the **potential value** against **emerging risks**?

**Question for regulators:** How to act and when to act?
Emerging risks to consumers from data use

Drivers
- Theft and loss
- Discrimination
- Obstructed consent
- Lack of anonymisation
- Unauthorised sharing and use
- Poor encryption
- Error
- Sabotage

Loss of privacy

Financial loss

Reputational risk

Manipulation

Safety and security

Exclusion and exploitative pricing

Source: Based on AIG, 2013; Armerding, 2017; Isaca, 2012; Newman, 2002; Ovelami, 2014; Uydess et al., 2018
How is this relevant for insurance regulators?

- New data can open new markets for underserved.
- New data approaches allows more targeted risk pricing – risk pooling breaks down and risks excluding customers.
- Data abuses increasingly prevalent – data privacy, financial loss, reputational loss and manipulation of choice.

How urgent?

- Insurers already collect and store a lot of sensitive personal information on their customers.
- Partnership and data sharing common and set to further increase, e.g. health wearables, social scoring, social media, location tracking

It is important for regulators to understand and prepare accordingly
Data protection and privacy legislation worldwide

Percentage of UN countries with or without current or pending privacy legislation

Source: UNCTAD 2018
**How are countries currently dealing with this?**

<table>
<thead>
<tr>
<th>Data protection regulatory approaches</th>
</tr>
</thead>
<tbody>
<tr>
<td>No policy and no regulation</td>
</tr>
<tr>
<td>- No constitutional protection of the right to privacy and no laws or regulation governing consumer data protection.</td>
</tr>
<tr>
<td>Policy but no regulation</td>
</tr>
<tr>
<td>- Constitutional protection of the right to privacy exists but no laws or regulation giving effect to the right as it pertains to personal data.</td>
</tr>
<tr>
<td>Sectoral regulation</td>
</tr>
<tr>
<td>- Data protection regulation determined and created on sector-by-sector basis.</td>
</tr>
<tr>
<td>- No overarching national or regional data protection legislation.</td>
</tr>
<tr>
<td>- E.g. USA, India and China</td>
</tr>
<tr>
<td>Omnibus regulation</td>
</tr>
<tr>
<td>- Overarching national or regional data protection legislation applies across sectors.</td>
</tr>
<tr>
<td>- May apply cross-border</td>
</tr>
<tr>
<td>- E.g. EU, New Zealand and Argentina</td>
</tr>
</tbody>
</table>

Source: Based on DLA Piper, 2018 and Deloitte, 2017
What role can insurance regulators play in dealing with these consumer risks?
What are the key factors for the insurance regulator to consider?

<table>
<thead>
<tr>
<th>Mandate</th>
<th>Country context</th>
<th>Cross-border implications</th>
<th>Key principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>• What is the insurance</td>
<td>• What is the specific country’s social norms and</td>
<td>• What are the implications of cross-border provision and</td>
<td>• What are the key principles to consider when regulating for the protection</td>
</tr>
<tr>
<td>regulator’s mandate?</td>
<td>policy relating to privacy and consumer data</td>
<td>regulation?</td>
<td>of consumer data in insurance?</td>
</tr>
<tr>
<td></td>
<td>protection?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• What is the nature of existing regulation?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Key principles

• **Data-handling requirements** e.g. restricting the collection of only certain specific data, only using it for a specific purpose and only storing it for a certain (specified) period.

• **Informed consent requirements**

• **Defining personal and sensitive data.**

• **Reasonable use:** use of consumer data only in the context of the use of the data for which consent was specifically provided, for the purpose of which the consent specified, and to the extent to which consent was given.

• **Security mechanisms** e.g. protection of consumer data by means of, for example, deanonymisation and encryption.
Thank you.

Follow us on Twitter @a2ii_org, Youtube and LinkedIn