United Nations Secretary-General's
Special Advocate for Inclusive Finance for Development

UNSGSA

Briefing on Data Privacy

By the UNSGSA's Fintech Sub-Group on Data Privacy

Why is data privacy important for financial inclusion?

The use of data is fundamental for financial markets to work efficiently. Market actors, including financial service providers (FSPs), customers, and regulators collect data for their varied needs. The vastly increasing quantity of data generated every day enables personal data and data from multiple sources to be combined to support the delivery of financial services. This data may include assets and debts, where we travel, what we do, what we purchase, which can in turn reveal sensitive information about us, such as medical conditions and treatment. This presents both opportunities and risks.

Opportunities

- Providers can use data to better assess risk and develop more responsive products and services for financially excluded and underserved customers. For example, decisions about the credit-worthiness of unbanked individuals could be based on their utility payments.
- For regulators, more data could help them better monitor the market and thus promote more transparency and more competition.
- Shared information infrastructure can harness data in ways that provide a more complete customer picture to financial services providers.

Risks

- Not handling data properly may cause consumers to lose trust in new financial services.
- Inaccurate or biased information may result in applications being rejected erroneously or improperly.
- Sales to third party data brokers can facilitate abusive marketing practices.
- Shared information infrastructure creates new challenges in terms of data control, storage, protection and usage.

What are the challenges in the financial inclusion context?

- Many poor consumers are concerned about the privacy of their personal data. Addressing those concerns is likely to help maintain and expand financial inclusion efforts.
- Increasing consumers' comfort level with digital financial services (DFS) should help speed their adoption. For instance, it is important to address concerns that data will be used to promote fraud schemes or could subject people to criminal activity if their wealth is publicly known.
- Lack of traditional financial data could exclude people from lending opportunities.

What are some key data protection issues?

Cross-border data flows:

- The nature of electronic communications means that data protection will necessarily involve cross-border issues.
- Many countries are understandably concerned about how their citizens' data will be handled in other countries, particularly countries that do not offer rigorous data protections.
- One response has been a movement toward data localization, prohibiting data from leaving the country so that it is not subject to surveillance authorities in other countries.
- While this is understandable, it could also lead to reduced competition and added costs for digital financial services.

Cyberattacks:

- DFS systems are vulnerable to cyberattack. Indeed, they can be more vulnerable because transactions occur using less sophisticated devices over insecure transmission lines.
- Losses and data breaches in DFS could entrench the perception that it is insecure and inhibits financial inclusion efforts.

How can governments enhance data privacy?

- **Governments can build a digital infrastructure** that empowers consumers to decide what information they want to share with businesses. For example, India's digital locker allows people to store important documents, such as birth certificates, and control who has access to them.
- **Governments can develop new models for data protection.** The notice and consent model of data protection could be revisited. It is particularly ill-suited to countries with low levels of literacy and financial education. The challenge of providing notice is further exacerbated in places where many people still use feature phones that are not designed to display lengthy privacy notices. A different approach would be to limit businesses' use, disclosure, and retention of information to legally defined "legitimate purposes."
- **Governments can provide resources and support for existing regulators** to address data protection or fund new dedicated data protection agencies.
- **Governments can encourage private sector voluntary data protection efforts.** FSPs can lead from the front in developing practical approaches and advancing public-private partnerships.

Annex: Resources

Programs

Selected jurisdictions with promising approaches to data privacy

- ***The European Unions's General Data Protection Regulation (GDPR)*** - Regulation (EU) 2016/679
- ***The Council of Europe's Updated Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*** - CETS No. 108

Organizations involved in technical assistance and/or funding of relevant activities

- Bill and Melinda Gates Foundation
- CGAP
- Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ)
- Omidyar Network

Selected Experts

- Katharine Kemp, UNSW Sydney
- Louis De Koker, La Trobe Law School, La Trobe University, Australia
- David Medine, Consultative Group to Assist the Poor

Recommended Readings

CGAP. 2014. *Financial Inclusion and Development: Recent Impact Evidence.* Focus Note, Washington DC, USA.

CGAP. *Protecting Customers Initiative.*

Dalberg, Dvara and CGAP. 2017. *Privacy on the Line.* Washington DC, USA.

DLA Piper. 2017. *Data Protection Laws of the World* (2017 edition).

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ). 2017. *Selected Regulatory Frameworks on Data Protection for Digital Financial Inclusion.* Berlin, Germany.

European Union. 2016. *General Data Protection Regulation 2016/679.* Brussels, Belgium.

This note was drafted by David Medine of CGAP under the guidance of the office of the UNSGSA and with support from Ant Financial, Better Than Cash Alliance, IFC, and McKinsey & Company.