भारतीय प्रबंध संस्थान बेंगलूर
INDIAN INSTITUTE OF MANAGEMENT
BANGALORE

sflc.in

# Concept Note: The Advent of AI in Fintech - Privacy, Security and Governance

IIM Bangalore and SFLC.in have been conducting a series of workshops on issues of technology and society. These workshops are being conducted at IIM Bangalore and cover contemporary aspects of technology in society such as regulations, governance, privacy, data protection, ethics and many others. The purpose of the workshops is to bring together key stakeholders - business managers, entrepreneurs, policy makers, academics, users and government - to comment on new phenomena and trends in technology use such as Artificial Intelligence, Machine Learning, Data Mining etc. in society. Each workshop focuses on some new technology or a key domain of technology use and bring together relevant actors. The outcome of the workshops will be policy documents that will be widely disseminated.

## Data Security Challenges in Fintech

The financial sector is becoming strategically focused and technologically advanced to respond to consumer expectations. The traditional methods have metamorphosed to utilities that are just a click away. The term "Fintech" encompasses all the new applications, processes, products or business models in the financial services industry and provided an end-to-end process through Internet and all the channels of delivery. Fintech establishes the partnerships between traditional financial institutions and contemporary businesses to help consumers get better and faster services. Seamless data sharing that forms the backbone of such partnerships brings in a fair share of threats and uncertainties. Security and privacy are the top threats to the rise of fintech. Some examples to cite are as below.

The "Bangladesh Bank cyber heist" took place a couple of years back and made headlines all over. Dozens of fraudulent instructions were issued by security hackers via the SWIFT network to illegally transfer close to US $1 billion from the Federal Reserve Bank of New York account belonging to Bangladesh Bank. The more recent ones are the massive Capital One hack and the leakage of credit card data from the USA and South Korea. Not a day goes by without yet another data leak uncovered. While this is common across all industries, financial services firms are reportedly hit by security incidents 300 times more frequently than businesses in other industries.

In the Indian context, although the fintech industry is still at a nascent stage, many startups have already emerged. E-wallets such as Paytm and MobiKwik, Citrus, PayUmoney and FreeCharge in payments, Policybazaar and Coverfox are a few well known names. India is poised to ride the fintech wave, with its young population, high internet subscription base, increasing household income, etc. Over the last couple of years, investments in fintech have grown rapidly (almost six times).

With more services online, data security is proving to be a major challenge. Some of this data also includes personally identifiable information and health information. Protecting this data and providing it to customers and third parties in a secure manner and when required are a challenge for the industry. The nature of threats and the concerns are quite varied. Some of the major security threats in the fintech world come from activities like – phishing, distributed denial of service (DDoS), man in the middle attacks (MIM attacks), malware etc.

In this workshop, we shall discuss how fintech companies need to be nimble and quick in updating their existing technology and adding new solutions in order to stay ahead of the threats and concerns related to privacy. Options available through the use of artificial intelligence/ machine learning, multi-factor authentication, bio-metric credentials, etc. should be discussed along with the challenges and biases the solutions would entail. In essence, the discussions should be around tackling the various limitations and concerns related to security and privacy through adoption of technology-based solutions that are contemporary, pragmatic and balanced.

**Advent of AI in Fintech**

Banking and financial services is one of the leading sectors when it comes to AI adoption. Existing and potential use of AI in this sector includes customer interaction through personalized engagement, virtual assistance, chat-bots, development of credit scores through analysis of bank history or social media data, and fraud analytics for proactive monitoring and prevention of various instances of fraud. AI in this sector has also been employed in wealth management - robo-advisory, algorithmic trading and automated transactions [1].

Since AI technology is heavily reliant on the collection and processing of personal and non-personal data, issues of transparency and potential data bias are some of the critical challenges with respect to the application of these technologies. Our financial data is some of the most sensitive personal data we own and automated technologies which make decisions on

[1] extracted from NITI Aayog's – National Strategy for AI

everything from credit scores to fraud detection can pose a great risk to our privacy and financial worthiness.

We need a meaningful dialogue around the data and privacy risks posed by the new technologies and their impact on society. These issues are particularly more pertinent as we move towards a cashless society in India.

**Other Policy Factors**

In a circular dated April 6, 2018, the Reserve Bank of India (RBI) mandated all payment system providers to store all data related to payment systems within India. This strict data localisation mandate from the RBI came at a time when the prudence of data localisation as required by the Draft Personal Data Protection Bill, 2018 was being debated in policy circles across the country. It is imperative to assess how this data localisation mandate affects the business of payment system providers and the privacy of their users and what should be the policy outlook for a robust governance regime.

Recently, on September 13, 2019, the Ministry of Electronics and Information Technology (MeitY), constituted an expert committee for deliberating on a 'Data Governance Framework' which will comment on the governance of non-personal data in India. Non-personal data according to MeitY includes – community data, aggregated data, derived data, anonymous data, AI training data, etc. As the fintech sector makes use of large data bases of personal as well as non-personal data to deliver their services, for a comprehensive look at future financial policy in India, it will be key to discuss the ramifications of such a data governance framework on existing financial systems.

**The Workshop**

The proposed roundtable will be a meetup to bring together different stakeholders in the fintech space and brainstorm on the current landscape of using AI based tools for data security in the fintech industry, the road ahead and the legal regime governing the scenario. The objective is to foster a community wide participation and discussion, to share experiences on employing AI based tools for security in the fintech industry. The session will also focus on the anticipated effects and issues of the Draft Personal Data Protection Bill, 2018 in its current form and the data governance framework for non-personal data as envisioned by MeitY.