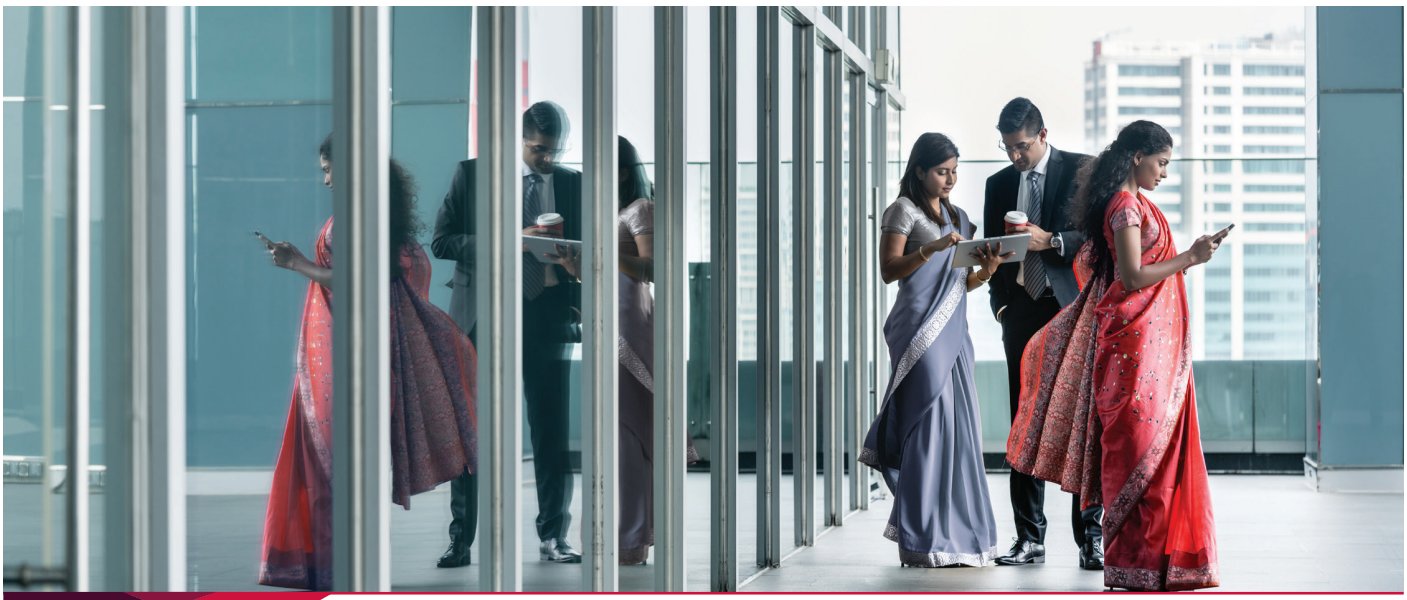
ESG *in Depth*

January 10, 2019

India's Evolving Data Privacy Regulation



- **Problem:** Digital transformation in India, driven by the development of a biometric ID system, has improved access to various products and services and helped businesses grow their customer bases. Unfortunately, data privacy and security improvements have not kept pace with the growth of technology adoption.
- **Development:** India is developing a General Data Protection Regulation (GDPR)-type law to hold businesses and government accountable for data breaches and the misuse of consumer data, and the Indian Supreme Court recently banned businesses from using and storing customer biometric identification.
- **Materiality:** Many Indian companies have benefited from lower customer acquisition costs (CAC) and improving margins by building their technology platforms around easy access to customer data using the free government biometric system, but have not sufficiently safeguarded or responsibly used this data. As a result, new data privacy laws could increase costs, create the risk of large fines and lead to reputational damage.
- **Next steps:** The widespread adoption of technology in India has the potential to lift millions of people out of poverty. While data privacy concerns should not stop us from investing in companies developing technologies that use and monetize personal information, they remain a material risk. Questions regarding these risks should be an important part of our engagements with management teams and will shed additional light on a company's operational quality.

ESG *in Depth*

January 10, 2019

Problem

The development of a biometric ID system by the Indian government has been transformational for businesses and individuals. More than 1.2 billion Indians are currently enrolled in Aadhaar, the largest biometric database in the world. Aadhaar is an identity program that assigns every individual a 12-digit number linked to his or her biometric and demographic data including his or her name, address, gender and date of birth along with a facial photograph, two iris scans, 10 fingerprints and, optionally, his or her mobile telephone number and email address. Aadhaar offers many benefits, such as

- tracing the distribution of government subsidies and benefits to end recipients
- enabling businesses to use the biometric ID to perform e-KYC (know your customer) and offer services such as two-minute online loan processing
- increasing access to financial and health care services for rural citizens

Many businesses have been created using a free software system built on Aadhaar infrastructure called India Stack. Sixty-nine percent of Indian tech startups are performing e-KYC via this platform. Some larger, established companies have also linked all their internal systems to Aadhaar data.

Unfortunately, data security infrastructure has not kept pace with the adoption of Aadhaar. Data privacy and security practices at most leading Indian organizations are weak, with little management focus or understanding of the topic and no real data-breach management mechanisms. Most organizations freely share data with third-party vendors, store biometric information on their servers and link customer IDs to sensitive information such as bank accounts, phone numbers and addresses. These practices make stolen data much more valuable to hackers and there have been a number of breaches, most of which have gone unreported because there has been no legal requirement to report them. This systemic weakness can be attributed largely to regulatory inertia: In 2016, 3.2 million debit cards were hacked with no meaningful legal repercussions.

Development

A government-appointed "Committee of Experts," led by retired Supreme Court justice B.N. Srikrishna, has developed a draft data protection bill that is very similar to the GDPR in Europe. More important, there now seems to be a will to *enforce* it. The premise of the report, release by the Srikrishna Committee in conjunction with the draft bill, is that "India must formulate a legal framework relating to personal data that can work as a template for the developing world." Key tenets of the bill include

- requirements to report data breaches to the newly created Data Protection Authority (DPAI)
- compliance by organizations handling Indian data even if located outside India
- individual consent before collecting sensitive personal data
- more stringent requirements for "significant" data processors
- Penalties of up to 4% of global revenue
- Data localization requirements (similar to Russia and China)

While this bill will improve personal data protection, it is not without its flaws. For example, the DPAI (whose directors will be appointed by the government) will decide what constitutes "sensitive data" that organizations may or may not be allowed to process for "reasonable purposes." The DPAI's definitions of these terms are discretionary and may create case-by-case disputes, which could be expensive and cumbersome to solve.

The Supreme Court's willingness to enforce this privacy law differentiates India from other Southeast Asian countries that also have their own draft legislations. This is evidenced by a recent Supreme Court of India ruling whereby private companies are no longer allowed to 1) require customers to share Aadhaar data with them, 2) store Aadhaar data on their servers or 3) use Aadhaar data for any purpose other than identity verification.

This is significantly disruptive to companies that, prior to the ruling, had been requiring new and existing customers to share their Aadhaar ID, which was then integrated into the company's internal systems and used for faster e-KYC and cross-selling of products. The cost to a bank of enrolling a customer online via Aadhaar is 30 to 50 times lower than enrolling a customer at a physical branch.

ESG *in Depth*

January 10, 2019

Materiality

For businesses relying on free Aadhaar data, India's privacy law will likely slow growth and increase both customer acquisition and compliance costs; it could also result in reputational damage and fines for companies that mismanage consumer data.

Based on our evaluation of large, listed Indian companies (excluding the tech sector), banks and telecoms seem likely to be the most impacted by this new legislation. These two industries include some of the largest users of consumer data in India and both industries, having underinvested in data security, are unprepared to meet growing privacy requirements.

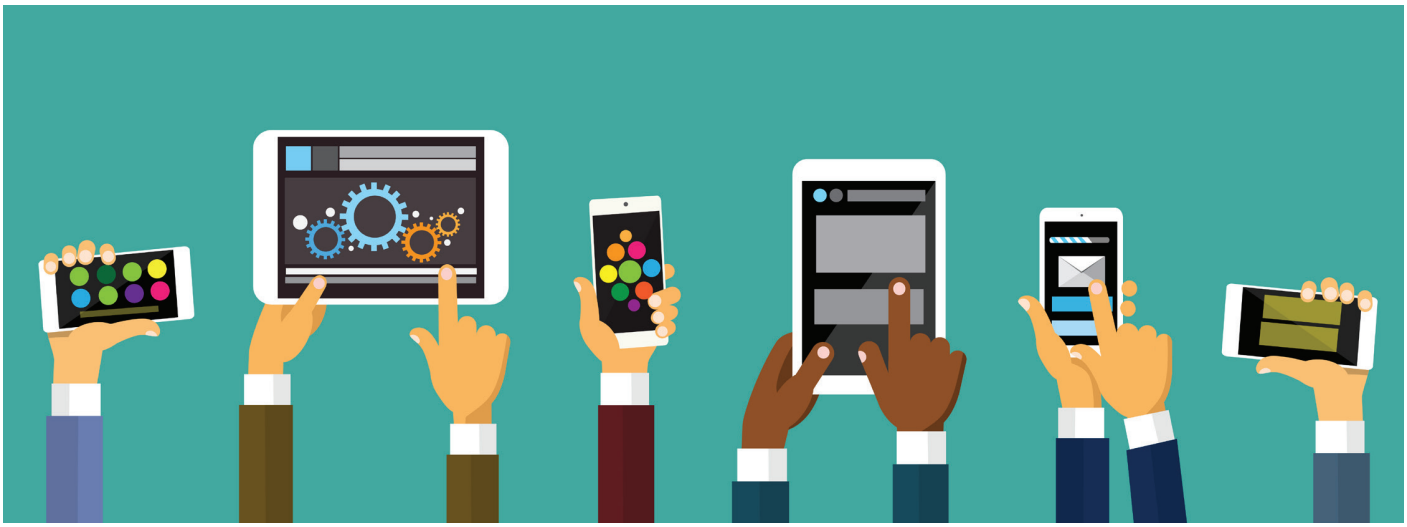
We took a closer look at banks to evaluate the preparedness of the sector. Our interviews with industry experts suggested that C-level understanding of data privacy and security is very weak, with little to no board awareness of the issue. Many companies lack basic security measures like data encryption and tokenization. Unsurprisingly, state-owned enterprises (SOEs) and non-banking financial companies (NBFCs) performed the worst. However, some private banks seem to be making meaningful investments to improve their data management practices in anticipation of upcoming regulatory changes. The banking sector has benefited from falling cost-to-income ratios due to declining CAC costs. This ratio should start to stabilize, if not reverse, as banks invest to secure consumer data. That said, incumbents who have used Aadhaar to build a critical mass of customers should continue to retain and widen their moat as rising compliance costs may impede less profitable disrupters.

Next Steps

Data management cannot be considered in isolation and is unlikely to drive an investment thesis on its own; however, management's approach to safeguarding consumer data can tell us a lot about a firm's culture and operational risk management.

Below are some suggestions for evaluating companies both in India and in other regions.

1. Use MFS' **ESG Sector Maps** to help you determine how material the issue of data privacy and security is for each industry/sector.
2. Evaluate each company's current security and privacy strategy and spend versus peers.
3. Assess management's understanding of the topic, using the questions in the **Data Privacy and Security Engagement Guide** that we have developed with the help of the MFS data security team.
4. Recognize the data privacy and security regulatory changes occurring in regions all around the world and consider modeling or valuing your names differently.



ESG *in Depth*

January 10, 2019

ESG *in Depth* is an internal research series produced for the benefit of MFS investment professionals. Although some **ESG** *in Depth* communications are made available externally to illustrate the thematic research regularly produced by and for our investment team, all suggestions in the document are directed at MFS investment professionals, not the general public.

Please keep in mind that a sustainable investing approach does not guarantee positive results.

The views expressed are those of the author(s) and are subject to change at any time. These views are for informational purposes only and should not be relied upon as a recommendation to purchase any security or as a solicitation or investment advice from the Advisor.

Distributed by:

U.S. MFS Investment Management; **Latin America** - MFS International Ltd.; **Canada** - MFS Investment Management Canada Limited. No securities commission or similar regulatory authority in Canada has reviewed this communication.

Please note that in Europe and Asia Pacific, this document is intended for distribution to investment professionals and institutional clients only.

U.K. - MFS International (U.K.) Limited ("MIL UK"), a private limited company registered in England and Wales with the company number 03062718, and authorized and regulated in the conduct of investment business by the U.K. Financial Conduct Authority. MIL UK, One Carter Lane, London, EC4V 5ER UK provides products and investment services to institutional investors. This material shall not be circulated or distributed to any person other than to professional investors (as permitted by local regulations) and should not be relied upon or distributed to persons where such reliance or distribution would be contrary to local regulation; **Singapore** - MFS International Singapore Pte. Ltd. (CRN 201228809M); **Australia/New Zealand** - MFS International Australia Pty Ltd (" MFS Australia") holds an Australian financial services licence number 485343. MFS Australia is regulated by the Australian Securities and Investments Commission.; **Hong Kong** - MFS International (Hong Kong) Limited ("MIL HK"), a private limited company licensed and regulated by the Hong Kong Securities and Futures Commission (the "SFC"). MIL HK is approved to engage in dealing in securities and asset management regulated activities and may provide certain investment services to "professional investors" as defined in the Securities and Futures Ordinance ("SFO"). **Japan** - MFS Investment Management K.K., is registered as a Financial Instruments Business Operator, Kanto Local Finance Bureau (FIBO) No.312, a member of the Investment Trust Association, Japan and the Japan Investment Advisers Association. As fees to be borne by investors vary depending upon circumstances such as products, services, investment period and market conditions, the total amount nor the calculation methods cannot be disclosed in advance. All investments involve risks, including market fluctuation and investors may lose the principal amount invested. Investors should obtain and read the prospectus and/or document set forth in Article 37-3 of Financial Instruments and Exchange Act carefully before making the investments.

MFSE-ESGID-NL-6/19
43301.2