PRIVACY INTERNATIONAL

Fintech: Privacy and Identity in the New Data-Intensive Financial Sector

November 2017

Fintech: Privacy and Identity in the New Data-Intensive Financial Sector

November 2017

~~PRIVACY~~
~~INTERNATIONAL~~

www.privacyinternational.org

Table of Contents

Executive Summary 4

Introduction 8

Part 1: The Promise and Power of Fintech 10

Part 2: Fintech and Identity 20

Part 3: The Growing Scope of Financial Identity 27

Conclusion: The Future of Fintech 38

A Way Forward for Privacy in the Fintech Sector 39

Executive Summary

Introduction

Financial services are changing, with technology being a key driver. It is affecting the nature of financial services, from credit and lending through to insurance, and even the future of money itself. The field of fintech is where the attention and investment is flowing. Within it, new sources of data are being used by existing institutions and new entrants. They are using new forms of data analysis. These changes are significant to this sector and the lives of people it serves.

With the promise of disruption, these changes in the financial industry have implications for human rights, privacy and identity. Fintech peers deeper into the lives of people. Many new services propose to increase the scope and nature of the data gathered about individuals. Data that people would consider as having nothing to do with the financial sphere, such as their text messages, is being used at an increasing rate by the financial sector. Yet protections are weak or absent.

It is essential that these innovations are subject to scrutiny. Much of the change serves the financial services industry and its interests. Financial services already have significant impacts on people, and fintech is an opportunity to expand financial inclusion to underserved regions. But fintech is also an expansion of the nature of financial services, and our financial identity, to cover more and more aspects of our lives. As a result, the perspective on fintech must be far broader than financial considerations.

About This Report

This report explores how developments in the fintech sector are posing issues for privacy. It is based on fieldwork interviews in India and Kenya.

The first part introduces the fintech sector, and interrogates some of the emerging narratives and discourses.

The second part explores in more detail the ways in which identity has become a central theme of fintech, through an examination of the developments in India surrounding the use of the Aadhaar identification number and how it relates to the India Stack initiative.

The third part looks in more detail at how data from more and more sources is being used to learn about those digital identities, focusing on the case of credit in Kenya.

Part 1: The Promise and Power of Fintech

Fintech covers a broad array of sectors and technologies. A non-exhaustive list includes:

- Alternative credit scoring (new data sources for credit scoring)
- Payments (new ways of paying for goods and services that often have implications for the data generated)
- Insurtech (the use of technology in the insurance sector)
- Regtech (the use of technology to meet regulatory requirements).

Similarly, a breadth of technologies are used in the sector, including:

- Artificial Intelligence
- Blockchain
- Internet of Things
- Telematics and connected cars

There are also narratives that are dominant in the fintech sector, that must be challenged:

- Disruption
- Visbility
- User-centricity
- Inclusion

The focus of this report, however, is not any specific technology; rather, it is the broader themes that operate across the fintech field. In particular, one of the ways in which fintech can be conceptualised is in terms of the new sources of data that are being used, and the new ways in which this can be analysed.

The take-up, and potential influence of fintech is not limited to an elite group of early-adopter consumers in the markets of Europe. The opposite is true: a survey by Ernst & Young found that the use of fintech by consumers with access to the Internet in developing markets including Brazil, India, China, Mexico and South Africa was considerably higher than the global average.

However, globally, the context in which fintech operates varies greatly. For example, the great take-up of M-Pesa mobile money in Kenya was not replicated when it was launched in South Africa. The payments sector remains an important area of concern for the privacy implications it brings to everyday life. For example, when demonetisation in India resulted in almost 90% of the currency being removed from circulation, the digital alternatives all generated a large amount of data about the users.

Part 2: Fintech and Identity

This report explores the idea that at the heart of fintech lies the concept of a "financial identity". This simultaneously prioritises the knowledge of the person as a unique individual, and shapes their identity with ever more data.

The Aadhaar identity scheme in India was introduced in 2009: this has provided a 12-digit number for over a billion Indians. Its use has expanded to the private sector via the India Stack initiative. Developed by the volunteers at iSPIRT, India Stack is a set of application programming interfaces (APIs). An API is essentially the code that allows two computer programs to communicate with each other. All of these are enabled by Aadhaar authentication. As described on the India Stack website:

"India Stack is a set of APIs that allows governments, businesses, startups and developers to utilise an unique digital Infrastructure to solve India's hard problems towards presence-less, paperless, and cashless service delivery."

At the heart of this innovation lies people's data, part of the stated goal of making India "data rich".

Two particular layers of the stack to consider:

- **eKYC:** the "electronic Know Your Customer" layer, which has resulted in a change in the initial nature of the identity database, to enable third parties to retrieve biographical data from the ID database.
- **UPI:** apps like BHIM, which make use of UPI for payments between bank accounts, means that increasing amounts of data are being generated for something as simple as making payments.

Part 3: The Growing Scope of Financial Identity

There has been a massive growth in the amount and nature of the data that is gathered by financial institutions about individuals. Many new data sources feed into the creation of financial identities. This is particularly visible through an exploration of the increase in the scope of credit scoring, a context in which these financial identities are used to make judgements about people.

Take the example from Kenya, where the M-Pesa mobile money transfer service has been widely used, but also is a generator of data. This has been one source of data for fintech startups like Tala and Branch, who use it to provide lending. But they also take a broad range of data from the borrower's smartphone, including location, call records, and SMS messages. This results in them making decisions based on factors like how often a customer calls their mother—based on call records on the phone and the contents of SMSs. Other fintech startups include M-Kopa, who lend to repay on solar panels.

However, there are ways in which companies in the fintech space in Kenya fail to protect the data of their customers. Some gather data regularly, even when the customer is not using the service, and use this to improve their algorithmic decision-making. Customers lack control over their data. In some cases, the algorithms are developed far from Kenya, in California for instance. Similarly, the danger arises as to what happens when these companies are sold: the data of customers and ex-customers alike becomes another asset to sell with the company.

Social media is another source of data for companies in the fintech space. However, decisions are made not on just the content of posts, but rather social media is being used in other ways: to authenticate customers via facial recognition, for instance.

The Future of Fintech

Will the future of fintech be one in which more and more data is used to judge customers? If our starting point for fintech is one in which the notion that being "data-rich" is inherently desirable, then this is the future that we risk building.

But there can be alternatives. Rather, when we consider the fintech future that we want to build, our starting point should not be that it is acceptable to gather and analyse any data that people can; just because we have the capabilities to do this, does not mean that we should. Protecting the human right to privacy of people across the globe is an essential element of fintech.

Recommendations

The report ends with general recommendations, followed by sets of specific ones directed at specific actors. The general recommendations are:

- Protecting the human right to privacy should be an essential element of fintech.
- Current national and international privacy regulations should be applicable to fintech.
- Customers should be at the centre of fintech, not their product.
- Fintech is not a single technology or business model. Any attempt to implement or regulate fintech should take this diversity into account, and be based on the type of activities they perform, rather than the type of institutions involved.

Introduction

Financial services are changing, with technology being a key driver. It is affecting the nature of financial services from credit and lending through to insurance and even the future of money itself. The field known as "fintech" is where the attention and investment is flowing. Within it, new sources of data are being used by existing institutions and new entrants. They are using new forms of data analysis. These changes are significant to this sector and the lives of the people it serves.

We are seeing dramatic changes in the ways that financial products make decisions. The nature of the decision-making is changing, transforming the products in the market and impacting end results and bottom lines. However, this also means that treatment of individuals will change.

This changing terrain of finance has implications for human rights, privacy and identity.

First, it peers deeper into the lives of people. Many new services propose to increase the scope and nature of the data gathered about individuals. Data that people would consider as having nothing to do with the financial sphere, such as their text messages, is being used at an increasing rate by the financial sector. Yet protections are weak or absent.

Second, the nature of decision-making is changing. While the power of machine learning to make decisions is being utilised, the understanding of the consequences and dangers of these technologies is lagging behind. New forms of discrimination may yet arise as a result.

Third, there are broader social concerns that emerge from the growth of fintech. The scope of the sector is broadening. Concepts like identity, key to people's lives, will be influenced by the developments in this sector. In addition, a particularly worrying implication is how developments in fintech will result in the alteration of the behaviours of people.

It is essential that these innovations are subject to scrutiny. Much of the change serves the financial services industry and its interests. Financial services already have significant impacts on people's lives. Fintech is an expansion of the nature of financial services, and our financial identity, to cover more and more aspects of our lives. As a result, the perspective on fintech must be far broader than financial, or even economic.

ABOUT THIS REPORT

This report explores how developments in the fintech sector are posing issues for privacy. It is based on fieldwork interviews in India and Kenya.

The first part introduces the fintech sector, and interrogates some of the emerging narratives and discourses. The second part explores in more detail the ways in which identity has become a central theme of fintech, through an examination of the developments in India surrounding the use of the Aadhaar identification number and how it relates to the India Stack initiative. The third part looks in more detail at how data is being used from more and more sources to learn about those digital identities, focusing on the case of credit in Kenya.

Part 1: The Promise and Power of Fintech

What is 'Fintech'?

The term 'fintech' has been defined by PricewaterhouseCoopers (PwC) as: "a dynamic segment at the intersection of the financial services and technology sectors where technology-focused start-ups and new market entrants innovate the products and services currently provided by the traditional financial services industry."[1]

Thus, the term sets up a dichotomy. As the Financial Times noted, the "table football, comfy sofas, book shelves and exposed brick walls"[2] of a *tech* startup contrasts with the corporate environment of *financial* institutions. This places 'fintech' and the 'traditional' financial sector in opposition with each other, with fintech firms being a threat to traditional banking[3] and financial services more generally.

Fintech covers a wide array of sectors and technologies[4]. A non-exhaustive list includes:

Alternative credit scoring: one of the focuses of this report, this is the use of new and different data sources, beyond the traditional credit file, for determining the risk of credit.

Payments: there is a move towards alternatives to cash, both for individuals paying shops and businesses and for the transfer of money between individuals. The consequences of some implementations of the alternatives to cash are discussed in this report.

Insurtech: the use of technology within the insurance industry, by established firms as well as startups[5]. This includes, for example, the insurance company Admiral's aborted plans to use Facebook posts to assess the risks of young drivers[6].

Regtech: the use of technology to help financial institutions meet their regulatory requirements[7], including building broad datasets of swathes of the population[8].

[1] PwC (2016) "Blurred lines: How FinTech is shaping Financial Services: Global FinTech Report March 2016": page 3 https://www.pwc.se/sv/pdf-reports/blurred-lines-how-fintech-is-shaping-financial-services.pdf

[2] "Fintech start-ups put banks under pressure", Financial Times, 12th September 2016 https://www.ft.com/content/ce8fa350-737f-11e6-bf48-b372cdb1043a

[3] See, for example, Bunea, S., Kogan, B & Stolin, D. (2016), "Banks Versus Fintech: At Last, it's Official" in The Capo Institute Journal of Financial Transformation, no. 44 http://www.capco.com/insights/capco-institute/~/media/Capco/uploads/articlefiles/file_0_1479208618.pdf

[4] For example, see the taxonomy presented here: World Economic Forum & Deloitte (2015) "The Future of Financial Services: How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed" http://www3.weforum.org/docs/WEF_The_future__of_financial_services.pdf

[5] Accenture (2017) "The Rise of Insurtech: How Young Startups and a Mature Industry Can Bring Out the Best in One Another" https://www.accenture.com/t00010101T000000__w__/gb-en/_acnmedia/PDF-50/Accenture-Insurtech-PoV.pdf

[6] Fisher, T. (2017) "Social media intelligence and profiling in the insurance industry: it's not only the price you pay that will be affected", Privacy International https://privacyinternational.org/node/1441

[7] Deloitte (2016) "RegTech is the new FinTech: How agile regulatory technology is helping firms better understand and manage their risks" https://www2.deloitte.com/ie/en/pages/financial-services/articles/RegTech-is-the-new-FinTech.html

[8] "VICE News Reveals the Terrorism Blacklist Secretly Wielding Power Over the Lives of Millions", VICE news, 4th February 2016, https://news.vice.com/article/vice-news-reveals-the-terrorism-blacklist-secretly-wielding-power-over-the-lives-of-millions

There is breadth in the technologies involved in the fintech industry. The industry makes extensive use of the data made available from technologies such as the smartphone and social networks, but it also makes use of new developments in the computer science/data analytics space. The new technologies that are being used, or are on the horizon, in this sector include:

AI: The term 'Artificial Intelligence' (AI) refers to a range of technologies, but in this context machine learning is the most relevant. Machine learning uses algorithms trained with vast amounts of data to improve a system's performance at a task over time. AI is used to profile people based on data from devices, networks and platforms, and to make consequential decisions on their lives[9].

Blockchain: Blockchain, or distributed ledger technology, is still best known for cryptocurrencies like BitCoin. However, the technology is being used more broadly, such as the World Bank-backed initiative in Kenya for blockchain-backed bonds[10]. Yet it is also used in other fields, like the push in digital identities[11]. A controversial example of this was a very small-scale scheme in the UK to pay benefits using blockchain technology, via an app developed by the fintech GovCoin[12] (since renamed DISC). The trial raised concerns, with the BBC reporting a former member of the Government Digital Service describing this as "a potentially efficient way for Department of Work and Pensions to restrict, audit and control exactly what each benefits payment is actually spent on, without the government being perceived as a big brother"[13].

Internet of Things: The Internet of Things is the network of sensor-equipped objects; this can range from wearable devices to smart toys and connected fridges. This is an area that is of growing relevance in the insurance industry. Its worth has already been proven, according to Ernst & Young (EY): "Early adopters have established a clear and compelling value proposition by demonstrating how data from in-home and automotive sensors, wearable technology, drones, GPS, mobile and telematics devices, networked appliances and multiple other sources can help grow new business, improve risk assessment and proactively engage policyholders in loss prevention."[14]

Telematics and connected cars: With an increasing number of sensors being built into cars, they are increasingly 'connected' and communicating with actors including

[9] Kaltheuner, F. and Polatin-Reuben, D. (2017) "Submission of evidence to the House of Lords Select Committee on Artificial Intelligence", Privacy International https://privacyinternational.org/sites/default/files/Submission%20of%20evidence%20to%20the%20House%20of%20Lords%20Select%20Committee%20on%20Artificial%20Intelligence%20-%20Privacy%20International.pdf

[10] "World Bank to Support Blockchain Bonds Trial in Kenya", coindesk, 2nd May 2017 https://www.coindesk.com/world-bank-to-support-blockchain-bonds-trial-in-kenya/

[11] "Accenture, Microsoft team up on blockchain-based digital ID network", Reuters, 19th June 2017 https://uk.reuters.com/article/us-microsoft-accenture-digitalid-idUKKBN19A22B

[12] "Use of bitcoin tech to pay UK benefits sparks privacy concerns", Financial Times, 12th June 2016 https://www.ft.com/content/33d5b3fc-4767-11e6-b387-64ab0a67014c?mhq5j=e3

[13] "Blockchain and benefits – a dangerous mix?" BBC News website, 14th July 2016 http://www.bbc.co.uk/news/technology-36785872

[14] EY (2016) "The Internet of Things in insurance: Shaping the right strategy, managing the biggest risks" http://www.ey.com/Publication/vwLUAssets/EY_-_The_internet_of_things_in_insurance/US$FILE/EY-the-internet-of-things-in-insurance.pdf

manufacturers, insurers and other vehicles[15]. Insurers are making use of this data to make decisions about the pricing of insurance, looking for features like sharp acceleration and braking, and time of day[16]. This raises privacy concerns: movements can be tracked, and much about the driver's life derived from their car-use patterns.

The focus of this report, however, is not on any specific technology; rather, it is the broader themes that operate across the fintech field. In particular, one of the ways in which fintech can be conceptualised is in terms of the new sources of data that are being used, and the new ways in which this can be analysed. This study illustrates some of the ways in which these sources of data are becoming increasingly intrusive, and are often analysed without appropriate protections in place. This has serious implications for privacy in the future.

Fintech in the Global Context

The take-up, and potential influence of fintech is not limited to an elite group of early-adopter consumers in the markets of Europe. The opposite is true: a survey by Ernst & Young found that the use of fintech by consumers with access to the Internet in developing markets including Brazil, India, China, Mexico and South Africa was considerably higher than the global average[17]. This, the report finds, is not surprising: these are places with high numbers of technologically-literate individuals, who are underserved by existing financial services[18].

Globally, the context in which fintech operates varies greatly. An example of this is the experience of Kenyan telecommunications giant Safaricom's M-Pesa mobile-based money transfers in different countries in Africa. Launched in Kenya in 2007, the M-Pesa service has proven massively successful, with 237 million person-to-person transactions taking place in 2013[19]. With the service reaching its tenth birthday, Safaricom stated that M-Pesa has generated more than US$1 billion, and generated 860,000 jobs[20]; whether this account is accurate or not, the ubiquity and social change potential of M-Pesa cannot be dismissed easily. Contrast this with the experience of launching M-Pesa in South Africa. In 2010, Vodacom partnered with Nedbank to launch M-Pesa in South Africa. But, with only 76,000 active users in South Africa, Vodacom announced its closure in 2016[21]. The *revolutionary* money transfer system of M-Pesa failed to get a hold on the South African market.

[15] Weatherhead, C. (2017) "Is your car connected?" Privacy International https://www.privacyinternational.org/node/1430

[16] "The big data of bad driving, and how insurers plan to track your every turn", Washington Post, 4th January 2016 https://www.washingtonpost.com/amphtml/news/the-switch/wp/2016/01/04/the-big-data-of-bad-driving-and-how-insurers-plan-to-track-your-every-turn/

[17] EY(2017) "EY FinTech Adoption Index 2017: The rapid emergence of Fintech", Page 7 http://www.ey.com/Publication/vwLUAssets/ey-fintech-adoption-index-2017/US$FILE/ey-fintech-adoption-index-2017.pdf

[18] EY(2017) "EY FinTech Adoption Index 2017: The rapid emergence of Fintech", Page 7 http://www.ey.com/Publication/vwLUAssets/ey-fintech-adoption-index-2017/US$FILE/ey-fintech-adoption-index-2017.pdf

[19] "M-Pesa and the rise of the gloval mobile money market", Forbes, 12th August 2015 https://www.forbes.com/sites/danielrunde/2015/08/12/m-pesa-and-the-rise-of-the-global-mobile-money-market/#21682f325aec

[20] "Safaricom's CEO: A decade on, M-Pesa has room to grow", The Africa Report, 2nd March 2017 http://www.theafricareport.com/East-Horn-Africa/safaricoms-ceo-a-decade-on-m-pesa-has-room-to-grow.html

[21] "Why M-Pesa failed in South Africa", BBC News website, 11th May 2016 http://www.bbc.co.uk/news/world-africa-36260348

Of course, practitioners in fintech are well-aware of some of the differences; for example, the companies operating in Kenya contacted in this research were looking to expand to other markets, but at the same time faced challenges of the changing circumstances.

The discourse on fintech from the financial sector too frequently ignores the broader political, economic and historical contexts in which particular fintech initiatives emerge.

Fintech and Payments

The payments sector is a key area of growth in the fintech sector: in 2016, this sector received 40% of the total investment in fintech[22]. Transactions paid by most electronic means can be tracked, even those in physical shops. In the US, Google has access to 70% of credit and debit card transactions—through Google's "third-party partnerships", the details of which have not been confirmed[23]. The growth of alternatives to cash can be seen all over the world, for example M-Pesa mobile money in many African nations.

There is a concerted effort against cash from elements of the development community. The Better Than Cash Alliance, for example, describes itself as "a partnership of governments, companies, and international organizations that accelerates the transition from cash to digital payments in order to reduce poverty and drive inclusive growth."[24] It is based at the UN, with funders that include the Bill & Melinda Gates Foundation, USAID, Omidyar Network, and several financial institutions which would appear to have an interest in promoting 'cashless' solutions: Citi Foundation, MasterCard, and Visa Inc[25]. The Alliance is pushing for digital payments as an alternative to cash.

A disturbing aspect of the cashless debate is the emphasis on the immorality of cash—and, by extension, the immorality of anonymity. A UK Treasury minister, in 2012, said that paying tradesman by cash was "morally wrong"[26], as it facilitated tax avoidance. Interested actors are more ready to criticise the anonymity of digital currencies such as bitcoin than they are to criticise cash. MasterCard states: "Contrary to transactions made with a MasterCard product, the anonymity of digital currency transactions enables any party to facilitate the purchase of illegal goods or services; to launder money or finance terrorism; and to pursue other activity that introduces consumer and social harm without detection by regulatory or police authority."[27] Ultimately, however, the argument about the moral depravity of anonymity applies equally to cash.

[22] "Global FinTech Funding Reached US$36 Bn in 2016 With Payments Companies Securing 40% of Total Funds", Let's Talk Payments 2nd January 2017, https://letstalkpayments.com/global-fintech-funding-36-bn-2016/

[23] "Google plans to track credit card spending", BBC News, 26th May 2017, http://www.bbc.co.uk/news/technology-40027706

[24] "About The Better Than Cash Alliance", Better Than Cash website, https://www.betterthancash.org/about

[25] They also have dozens of governments and international organisations as partners. See https://www.betterthancash.org/members/company

[26] "Paying tradesmen cash in hand morally wrong, says minister", BBC News, 24th July 2012, http://www.bbc.co.uk/news/uk-18964640

[27] "MasterCard rails against Bitcoin's anonymity", Computer World, 2nd December 2014, https://www.computerworld.com.au/article/560825/mastercard-rails-against-bitcoin-anonymity/

Fintech Narratives

There is a set of dominant narratives that permeate the fintech concept. These are used by start-ups themselves, governments, and the associated industry writing on fintech for consultancies and media. It is essential to critically analyse these narratives to understand the changing nature of individual rights, including privacy, going forward; just as understanding Silicon Valley's dominant narratives around investment-led innovation and *free* services that could pivot to new uses, links strongly with data-driven advertising models, the consolidation onto centralised platforms, and the emergence of data as the fuel for algorithms for expansive purposes.

Disruption: *"FinTech is all about innovation, disruption and transformation"* [28], as PwC puts it. The notion here is that fintech brings change that will alter the nature of the way in which the financial services industry operates. This change runs throughout the industry: "Every bank on the planet is currently wrestling with some sort of innovation agenda in response to FinTech encroachment and the disruptive innovations they have brought to the financial services market over the last decade"[29].

The tech startup field, beyond fintech, has a deep love-affair with the notion of 'disruption': the concept runs through much of the field, but it is not a concept with which there has been critical engagement[30]:

> **"Most big ideas have loud critics. Not disruption. Disruptive innovation as the explanation for how change happens has been subject to little serious criticism, partly because it's headlong, while critical inquiry is unhurried; partly because disrupters ridicule doubters by charging them with fogyism, as if to criticize a theory of change were identical to decrying change; and partly because, in its modern usage, innovation is the idea of progress jammed into a criticism-proof jack-in-the-box."**
>
> J. Lepore in The New Yorker, June 2014

It is important, then, to understand the limitations of the concept of 'disruption' within the fintech space. It becomes easier to describe it in terms of what it is not: it is not necessarily a revolutionary change in the nature or ownership of the financial services industry. As is illustrated with the examples in this research, the goal of many fintechs is to be sold; quite possibly, this will be to existing players within the market. This also means that the early adopters' data could be integral to the sale.

[28] PwC (2017) "Redrawing the lines: FinTech's growing influence on Financial Services" https://www.pwc.com/gx/en/industries/financial-services/fintech-survey/report.html

[29] McAleavey, C. (2017) "Disruptive Financial Technology and the Innovator's Dilemma", leveris http://blog.leveris.com/disruptive-financial-technology-and-the-innovators-dilemma/

[30] Lepore, J. (2014) "The disruption machine: What the gospel of innovation gets wrong." In The New Yorker, 23rd June 2014 http://www.newyorker.com/magazine/2014/06/23/the-disruption-machine

This is not to deny that changes are being brought about by the introduction of fintech, and the developing alterations in how we think about key issues like identity and data. There are shifts occurring in the relationship between a customer and their bank, and in the ways in which identity and data are used. However, the issue with the disruption narrative is the assumption that these changes are positive for the individual or communities more broadly. From their perspective, we cannot assume that that all such changes are positive to the customer's experience or, indeed, their human rights.

Visibility: Fintech Makes Visible Those Who Are Invisible to the Financial Sector

In this development-focused narrative, the promise of fintech is to make previously-underserved populations "visible". This often applies to those who lack a formal credit file, and thus are likely to have no existing "financial identity". New data sources mean that these people develop a financial identity. As the Omidyar Network describes it, "these trends are helping to change the landscape on inclusion and reach, offering the promise that billions of previously 'invisible' consumers can be 'visible' for the first time."[31]

This visibility narrative needs exploring. Professors Linnet Taylor and Ralph Schroeder describe how the notion of visibility has positive *and* negative effects:

"Greater visibility of populations can have positive effects, as when GDP is measured more accurately, or the spread of disease tracked faster, or relief brought to disaster areas where needed. On the other hand, visibility can lead to marketing that pesters users, fleeing populations can be targeted by militaries that pursue them, or visible populations may be favoured at the expense of less visible ones."[32]

Another point about visibility is highlighted by a recent report on the use of the Internet by LGBTQ activists in Kenya and housing activists in South Africa[33]. These activists are careful of how visible they are online, as they can feel at risk if they go public. On the other hand, making the activities of others visible—like through highlighting violence and blackmail against LGBTQ people—can become an important advocacy tool. These examples highlight the issues surrounding politics, power and visibility; it begins to draw into question the concept that "visibility" is inherently inclusive and empowering.

For instance, Indian media reported that an Indian loan provider uses the information on an individual's Twitter profile to determine loan eligibility:

"If someone is politically active and engages in political campaigns, which are visible

[31] Omidyar Network (2016), "Big Data Small Credit: The Digital Revolution and It Impact on Emerging Market Customers", page 6, https://www.omidyar.com/sites/default/files/file_archive/insights/Big%20Data,%20Small%20Credit%20Report%202015/BDSC_Digital%20Final_RV.pdf

[32] Taylor, L. and Shroeder, R. (2015) "Is bigger better? The emergence of big data as a tool for international development policy", in GeoJournal Volume 80 Issue 4, https://link.springer.com/article/10.1007/s10708-014-9603-5

[33] Ganesh, M.I.; Deutch, J. and Schulte, J. (2016) "Privacy, anonymity, visibility: dilemmas in tech use by marginalised communities", https://opendocs.ids.ac.uk/opendocs/handle/123456789/12110

through their social media profiles, it is not a good sign since we do not want to go through the hassles that may come up in collection. It shows that the person can raise issues at the time of collection in these political groups"[34].

An alternative, but related concept to "visibility" is the historian James Scott's term "legibility". Scott writes on the role of vernacular names:[35]

> **Vernacular naming practices throughout much of the world are enormously rich and varied. In many cultures, an individual's name will change from context to context, and within the same context, over time. It is not uncommon for a newborn to have had one or more name changes in utero in the event the mother's labour seemed to be going badly. Names often vary at each stage of life (infancy, childhood, adulthood, parenthood, old age) and, in some cases, after death. Added to these may be names used for joking rituals, mourning, nicknames, school names, secret names, names for age-mates or same-sex friends, and names for in-laws. Each name is specific to a phase of life, a social setting, or a particular interlocutor. To the question, "What is your name?" the reply in such cases can only be: "It depends."**
>
> James Scott

Scott's work focuses on the state, arguing that the state "requires the capacity to locate citizens uniquely and unambiguously"[36]. Financial institutions have very similar needs; the need to identify customers. Legibility, Scott argues, is about the state being unable to comprehend the complexity of the social world, developed in local situations and full of a breadth of local meaning. Thus, a state attempts to organise people and society in a rational, optimised manner.

The advantage of thinking about the concept of "legibility" over "visibility" is twofold. First, it emphasises the role of the observer: visibility as a concept rarely goes along with an answer to the question, "visible to whom?". Secondly, it emphasises how the collection of data can alter the subject; it is not a neutral act, but one filled with power dynamics.

[34] "The new lending game, post-demonetisation", ET Tech, 6th January 2017, http://tech.economictimes.indiatimes.com/news/technology/the-new-lending-game-post-demonetisation/56367457

[35] Scott, J., Tehranian, J. and Mathias, J. (2002) "The Production of Legal Identities Proper to States: The Case of the Permanent Family", in Comparative Studies in Society and History, Vol. 44 No. 1, https://www.cambridge.org/core/journals/comparative-studies-in-society-and-history/article/the-production-of-legal-identities-proper-to-states-the-case-of-the-permanent-family-surname/BA957F9C274070A336A67C75CDA384C0

[36] Scott, J., Tehranian, J. and Mathias, J. (2002) "The Production of Legal Identities Proper to States: The Case of the Permanent Family", in Comparative Studies in Society and History, Vol. 44 No. 1, https://www.cambridge.org/core/journals/comparative-studies-in-society-and-history/article/the-production-of-legal-identities-proper-to-states-the-case-of-the-permanent-family-surname/BA957F9C274070A336A67C75CDA384C0

User-centricity: Another narrative running through the fintech sector is the "user-centric" nature of the design; the emphasis placed on the *ability for a customer to gain access to services quickly and easily, with a minimum of need for user input.*

In an example, the founder of the US-based start-up property insurance business Kin has written, "When it comes to financial services, most people don't want to think about it and the best thing I can do with tech is make it easier."[37] Rather than having a multi-page form to fill in to apply for property insurance, Kin only takes three clicks: most of the data that would normally have been provided by the applicant—like the construction materials of their home—are provided from more publicly-available sources.

Fintech is also designed to be fast for the borrower. The field has developed: back in 2012, the fintech pioneer Lenddo—before they became purely a scoring business—processed a loan application within one business day, with an additional business day to send the funds[38]. Nowadays, however, the sector's speed has increased. In the case of Kenyan lender Tala, the period has been reduced to two minutes[39].

As will be discussed below, this alleged simplicity of the decision-making process, or of the transaction, masks a hugely complex process occurring behind the scenes.

Inclusion: Financial Inclusion is Bringing New People into the Financial System

The World Bank is calling for Universal Financial Access by 2020; this involves the two billion people who do not currently have access to a basic bank account having such access by 2020[40]. Fintech is described by the World Bank as playing a role in this[41].

The centrality of "Financial Inclusion" is critiqued by the academics Gabor and Brooks, who argue that it places the emphasis on the individual rather than structural change to give people more access: "F[inancial] I[nclusion] as a development paradigm, therefore, envisages no material change in the (changing) structures that generate marginality, but rather seeks to channel individual behaviour, through digital surveillance and education, to engage and identify with these structures."[42] As a result, they argue, this sector is best understood not as part of an "inclusion/exclusion binary" but rather as a system of creating "new financial identities that conform to the requirement of expanding financial markets"[43].

[37] "With US$4 million in funding, Kin wants to change how homeowners get insured", TechCrunch, 1st August 2017, https://techcrunch.com/2017/08/01/kin-insurance/

[38] Frequently Asked Questions from the website of Lenddo dates 9th Deember 2013, available from the Wayback Machine at Archive.org: https://web.archive.org/web/20130129174319/https://www.lenddo.com/pages/faq

[39] "How Tala Mobile Is Using Phone Data To Revolutionize Microfinance", Forbes, 29th August 2016 https://www.forbes.com/sites/forbestreptalks/2016/08/29/how-tala-mobile-is-using-phone-data-to-revolutionize-microfinance/

[40] "UFA2020 Overview: Universal Financial Access by 2020", World Bank website, http://www.worldbank.org/en/topic/financialinclusion/brief/achieving-universal-financial-access-by-2020

[41] Miller, M. (2017) "Can 'fintech' innovations impact financial inclusion in developing countries?", World Bank blog, 12th April 2017 http://blogs.worldbank.org/psd/can-fintech-innovations-impact-financial-inclusion-developing-countries

[42] Gabor,D. and Brooks, S. (2016) "The digital revolution in financial inclusion: international development in the fintech era" in New Political Economy, Vol. 22, Issue 4, page 10 http://www.tandfonline.com/doi/abs/10.1080/13563467.2017.1259298

[43] Gabor,D. and Brooks, S. (2016) "The digital revolution in financial inclusion: international development in the fintech era" in New Political Economy, Vol. 22, Issue 4, page 9 http://www.tandfonline.com/doi/abs/10.1080/13563467.2017.1259298

Another potentially problematic area of the inclusion agenda is risks surrounding discrimination arising from algorithms[44]. One of the key dangers emerging from algorithmic decision-making—for example, determining eligibility for credit—is the risk that this algorithm discriminates. To an extent, these issues are not being seriously addressed by many in the fintech field; rather than interrogating the decision-making process to see if it is genuinely fair, the questions of discrimination are not issues that they have considered. These issues are particularly problematic in the diverse nature of potential discrimination that is possible amongst the emerging markets where much fintech growth lies.

Financial Identity

This report explores the idea that at the heart of fintech lies the concept of a "financial identity". This simultaneously prioritises the knowledge of the person as a unique individual, and shapes that identity with ever more data.

A 2016 report by the World Economic Forum (WEF) emphasised the importance of identity to financial services.[45] The report claimed that the lack of digital identities harms fintech, the financial services industry more broadly, and society as a whole. In turn, the authors argued that the financial services industry is ideally placed to lead the development of digital identity. According to this argument, financial institutions already store and verify customer identities and attributes, as well as having a commercial incentive to collect information that is accurate. These institutions have a broad reach, in some markets at least, and are already regulated and trusted. WEF concludes that financial institutions "should champion efforts to build digital identity systems, driving the building and implementation of identity platforms"[46].

If the financial industry is looking to build identity systems, and with their privileged status in societies to build comprehensive and widely used systems, then they may massively expand their power and influence. With changes in laws across the world, there is an increased requirement and reliance on individuals to identify themselves across their daily lives. If the financial sector drives this culture, that sector's assumptions, epistemology and concept of identity will become ubiquitous.

We urgently need a critical analysis of identity in the financial services industry. It is this industry that is producing many of the most interesting developments in the field of identity. These developments have consequences for privacy, in terms

[44] Barocas, S. (2014) "Data Mining and the Discourse on Discrimination", : in Proceedings of the Data Ethics Workshop: Conference on Knowledge Discovery and Data Mining; August 24th 2014, New York City, https://dataethics.github.io/proceedings/DataMiningandtheDiscourseOnDiscrimination.pdf and Barocas, S. and Selbst, A.D. (2016) "Big Data's Disparate Impact", in 104 California Law Review 671, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899

[45] World Economic Forum & Deloitte (2016) "A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity" http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

[46] World Economic Forum & Deloitte (2016) "A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity": page 28 http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

of the intrusiveness of the data which creates financial identities, as well as the consequences these identities have for privacy. This means that a focus on this emerging sector is particularly informative and valuable.

DEMONETISATION

On 8th November 2016, Prime Minister Narendra Modi of India announced that the two largest banknotes—constituting almost 90%[47] of the money supply—were being withdrawn from circulation. Indians had until December to change their money at a bank. Perhaps the only peacetime precedents to this move were times of hyperinflation or similar crises, like in Zimbabwe in 2015[48]. India was facing no such crisis.

The motives of this move remain a source of debate; the official line was that this was a "surgical strike… done on black money, terror funding and drug money", as the Defence Minister put it[49]. If this was the motive, then we must judge demonetisation a failure: ultimately, 99% of the old notes were exchanged at a bank, meaning that either the amount of "black money" in the economy was tiny, or that the "black money" in the economy was successfully laundered[50].

But demonetisation can also be understood as a push for the "digitisation" of India's economy. Indeed, Bill Gates—a notable proponent of digital payment methods—said shortly after the start of demonetisation, "India is pushing towards digitisation in a big way. The scale of the country means that once India gets there, the amount of digital innovation here will be greater than anywhere else in the world."[51] Gates said of the issues raised by demonetisation: "Government transitions are never managed perfectly and never easy" [52].

But the impact on how people interact with the economy is potentially far deeper. The alternatives to cash available were options like mobile wallets, including PayTM and JioMoney[53]. It also paved the way for options based on the UPI, as detailed below: Prime Minister Modi promoted the NPCI's own app, BHIM, only a few months after demonetisation at the end of 2016.

[47] "Why India wiped out 86% of its cash overnight", BBC News website, 14th November 2016, http://www.bbc.co.uk/news/world-asia-india-37974423

[48] https://qz.com/845803/demonetisation-zimbabwe-myanmar-and-ussr-have-been-there-done-that-and-screwed-themselves-over/

[49] "Demonetisation a surgical strike on black money, says Manohar Parrikar", Indian Express, 27th November 2016, http://indianexpress.com/article/india/india-news-india/demonetisation-surgical-strikes-modi-manohar-parrikar-4398447/

[50] "Demonetisation a surgical strike on black money, says Manohar Parrikar", Indian Express, 27th November 2016, http://indianexpress.com/article/india/india-news-india/demonetisation-surgical-strikes-modi-manohar-parrikar-4398447/

[51] "Bill Gates backs demonetisation, says it's worth the pain", Times of India, 18th November 2016 https://timesofindia.indiatimes.com/india/Bill-Gates-backs-demonetisation-says-digital-payments-can-transform-lives-of-poor/articleshow/55486066.cms

[52] "Bill Gates backs demonetisation, says it's worth the pain", Times of India, 18th November 2016 https://timesofindia.indiatimes.com/india/Bill-Gates-backs-demonetisation-says-digital-payments-can-transform-lives-of-poor/articleshow/55486066.cms

[53] Fisher, T. (2016) "The legacy of demonetisation: how India's cashless future threatens to erode citizens' privacy", Privacy International https://www.privacyinternational.org/node/1036

Part 2: Fintech and Identity

The Development of Financial Identity

The history of the creation of credit bureaus dates back to the 1840s, according to Josh Lauer[54]. Mercantile credit reference agencies collected extensive files on small business owners, collecting information from local news stories, rumour and anecdote. The agencies "invented what was not just a highly coordinated system of disciplinary surveillance, but the very idea of financial identity itself. This new technology of identification became a key infrastructural component of the modern credit economy and, in turn, produced its own category of social reality"[55]. This financial identity, Lauer argues, was not just the normative judgement on the character of the business-owners. Rather, it "offered the tantalizing possibility of rational calculation"[56]—credit reporting as part of the 19th century developments in statistics and accountancy. "The same ideals of objectivity and transparency that stimulated the quantification of populations, social phenomena, and commercial transactions were also manifest in the development of financial identity as a site of individual accountability."[57]

We can thus see the development of the credit agency in the context of the 19th century developments in *statistics*. Statistics, Ian Hacking argues, shaped social realities and the categories into which people fell, as well as facilitating the development of the bureaucratic apparatus of the state[58]. Thus, the developments of the 19th century served to shape the characterisation of people, and in particular served to give them an "objective" financial identity. They did not reflect the existing identities, but created them.

Just as the 19th century led to shifting notions of character, categorisation and financial identity, so must we see what changes the developments of the 21st have wrought. If fintech is as "disruptive" as claimed, it too must bring a change in how we conceive financial identity. We see the vast increase in "objective" sources of data, collected in unprecedented volume, analysed using new statistical techniques such as artificial intelligence and machine learning. How will these developments shape the financial identity of the future?

[54] Lauer, J. (2008) "From Rumor to Written Record: Credit Reporting and the Invention of Financial Identity in Nineteenth-Century America", in Technology and Culture, Volume 29 Number 2: pages 304-5, https://muse.jhu.edu/article/236961

[55] Lauer, J. (2008) "From Rumor to Written Record: Credit Reporting and the Invention of Financial Identity in Nineteenth-Century America", in Technology and Culture, Volume 29 Number 2: pages 304-5, https://muse.jhu.edu/article/236961

[56] Lauer, J. (2008) "From Rumor to Written Record: Credit Reporting and the Invention of Financial Identity in Nineteenth-Century America", in Technology and Culture, Volume 29 Number 2: pages 304-5, https://muse.jhu.edu/article/236961

[57] Lauer, J. (2008) "From Rumor to Written Record: Credit Reporting and the Invention of Financial Identity in Nineteenth-Century America", in Technology and Culture, Volume 29 Number 2: pages 304-5, https://muse.jhu.edu/article/236961

[58] Hacking, I. (1991) "How should we do the history of statistics?" in Buchell, G., Gordon, C., and Milller, P. The Foucault effect: studies in governmentality, University of Chicago Press, Chicago.

Who Are You? ID Systems and Fintech

Ideas of financial identity are a key aspect of fintech, but also have broader implications. This will be explored through a look at the case of the Aadhaar identity scheme in India.

Know Your Customer: KYC

"Know Your Customer"—KYC—is the process by which banks or other financial institutions identify their customers in order to evaluate the possible legal and other risks associated with doing business with them. According to the academic Daniel Mulligan, the origins of KYC, and anti-money laundering requirements, date (in the US at least) back to the "War on Drugs" in the 1970s[59]. Though the inter-governmental body which deals with KYC regulations, the Financial Action Task Force (FATF), was founded in 1989,[60] rules tightened significantly following the 9/11 attacks, and the subsequent "War on Terror".[61]

KYC, in the years following the tightening of anti-money laundering rules post-9/11, received criticism for leading to financial exclusion, particularly for the most vulnerable who frequently lacked documentation such as proof of address[62]. The approach to combating the funding of terrorism is risk-based, an approach that has been criticised[63]. Rather than judging the risk of each individual client, there has been a broader "de-risking" of whole sectors of the industry or groups of people who are high-risk and lower profit[64]. An example is remittances: in 2013, Barclays Bank closed the accounts of dozens of UK-based remittance companies, a move that disproportionately affected groups like migrant workers[65]. The risk-based approach is not about 'catching' people after the crime, but rather as an intelligence-gathering tool in itself, to detect future terrorist attacks[66]. It looks to do this in a way that does not disrupt the global economy[67]. The current discourse from FATF places more emphasis on financial inclusion than the earlier regime[68], but still retains the same risk-based approach.

[59] Mulligan, D. (1998) "Know Your Customer Regulations and the International Banking System: Towards a General Self-Regulatory Regime", in Fordham International Law Journal, Volume 22, Issue 5, http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1647&context=ilj

[60] "Who we are" FATF webpage, http://www.fatf-gafi.org/about/

[61] Amoore, L. and De Goede, M. (2005) "Governance, risk and dataveillance in the war on terror" in Crime, Law and Social Change, Volume 43, Issue 2-3, https://link.springer.com/article/10.1007/s10611-005-1717-8

[62] See, for example, the sources linked in Amoore, L. and De Goede, M. (2005) "Governance, risk and dataveillance in the war on terror" in Crime, Law and Social Change, Volume 43, Issue 2-3: pages 155-6 https://link.springer.com/article/10.1007/s10611-005-1717-8

[63] Amoore, L. and De Goede, M. (2005) "Governance, risk and dataveillance in the war on terror" in Crime, Law and Social Change, Volume 43, Issue 2-3, https://link.springer.com/article/10.1007/s10611-005-1717-8

[64] IFC (2016) "Mitigating the effects of de-risking in emerging markets to preserve remittance flows", https://www.ifc.org/wps/wcm/connect/68a895a7-dc34-48fd-9c80-215b0fdc6da4/Note+22+EMCompass+-+De-Risking+and+Remittances++FINAL.pdf?MOD=AJPERES

[65] IFC (2016) "Mitigating the effects of de-risking in emerging markets to preserve remittance flows", https://www.ifc.org/wps/wcm/connect/68a895a7-dc34-48fd-9c80-215b0fdc6da4/Note+22+EMCompass+-+De-Risking+and+Remittances++FINAL.pdf?MOD=AJPERES

[66] Amoore, L. and De Goede, M. (2005) "Governance, risk and dataveillance in the war on terror" in Crime, Law and Social Change, Volume 43, Issue 2-3, https://link.springer.com/article/10.1007/s10611-005-1717-8

[67] Amoore, L. and De Goede, M. (2005) "Governance, risk and dataveillance in the war on terror" in Crime, Law and Social Change, Volume 43, Issue 2-3, https://link.springer.com/article/10.1007/s10611-005-1717-8

[68] FATF (2013) "Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion" http://www.fatf-gafi.org/media/fatf/documents/reports/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf

Aadhaar in India

WHAT IS AADHAAR?

Aadhaar is India's system of identification, introduced in 2009. An Aadhaar number is a 12-digit number. The authority in charge of Aadhaar is the Unique Identification Authority of India (UIDAI)[69]. At Aadhaar registration, the biometrics of a person are taken: the fingerprints of all ten fingers, an iris scan of both eyes, and a photograph of the person's face[70]. The demographic details of the individual are also gathered, which require either supporting documentation (like a birth certificate or a proof of address)[71] or by introduction from the head of family or "introducer". In practice, however, only a tiny number of people applying for Aadhaar use the introducer system—0.03% of enrolments by 2015[72]—indicating that almost all of the people who applied for Aadhaar had existing identification. The biometric and biographical details of an individual are stored in the UIDAI's Central Identities Data Depository (CIDR).

India's Aadhaar identification scheme, as well as its role in the provision of benefits, also has a role to play in the financial sector. It forms a central role in what is called the JAM Trinity: the government initiative to limit leaks in government subsidies by linking three aspects: Jan Dhan bank accounts (for which the Aadhaar e-KYC plays a key role, see below); Aadhaar; and mobile[73].

Aadhaar has been praised by elements of the development community for its role in financial inclusion. For example, the Bill and Melinda Gates Foundation wrote: "India has been especially innovative about investing in the building blocks of digital financial inclusion. Aadhaar, a nationwide biometric identification system, makes it simpler and more secure for poor people to do business with banks."[74]

But it is important to understand how Aadhaar creates this financial inclusion: by the creation of vast amounts of personally-identifiable data. As the former chairman of the UIDAI, and the "father of Aadhaar"[75] Nandan Nilekani puts it, India will go "from being data poor to data rich"[76] in the next few years. At the heart of this is a plan for India Stack; as we shall see, its goal is to make India a "data-rich" nation[77].

[69] "About Aadhaar", UIDAI website, https://uidai.gov.in/your-aadhaar.html

[70] "About Aadhaar", UIDAI website, https://uidai.gov.in/your-aadhaar.html

[71] The enrolment form for Aadhaar can be found on the UIDAI website: https://uidai.gov.in/images/aadhaar_enrolment_correction_form_version_2.1.pdf

[72] "'Most Aadhar Cards Issued to Those Who Already Have IDs'", The Wire, 3rd June 2015, https://thewire.in/3108/most-aadhar-cards-issued-to-those-who-already-have-ids/

[73] Deloitte (2016) "Digital: A Revolution in the Making in India" https://www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-media-telecommunications/in-tmt-digital-revolution-in-making-cii-noexp.pdf

[74] Bill and Melinda Gates Foundation, (2017) "Goalkeepers: The Stories Behind the Data", page 18, http://www.globalgoals.org/goalkeepers/datareport/assets/downloads/Stories_behind_the_data_2017.pdf

[75] "'Show me even one example of data theft. Aadhaar is very, very secure'" Times of India, 2nd April 2017, https://timesofindia.indiatimes.com/home/sunday-times/all-that-matters/show-me-even-one-example-of-data-theft-aadhaar-is-very-very-secure/articleshow/57966495.cms

[76] Nilekani, N. (2016) "Forward" in Credit Suisse "India Financials Sector", https://research-doc.credit-suisse.com/docView?language=ENG&format=PDF&document_id=1062747711&source_id=emcsplus&serialid=Wm0zJuKszkmbCwRYV7hD9c7T64WOziu3Z51RrM7Zcs0%3D

[77] Presentation from ProductNation.in: "India Stack - Towards Presence-less, paperless and cashless service delivery. an iSPIRT initiative"

India Stack

IndiaStack describes itself as an "initiative" of iSPIRT—the Indian Software Product Industry Roundtable, a powerful think tank established in 2013[78]. India Stack is a set of application programming interfaces (APIs). An API is essentially the code that allows two computer programmes to communicate with each other. An API could be used, for example, to enable weather information from one provider to be used in another app. It is a Facebook API that allows an app to use Facebook to provide a login, and to subsequently access some data from a user's profile. APIs facilitate many of the developments in fintech across the globe—for example, it is a set of APIs that allow the credit scorer Lenddo to integrate its algorithms with a lender's website[79]. In the European context, the European Union's Payment Services Directive (PSD2) requires banks to have a set of APIs for other banks or portals to have access to customers' account data[80].

India Stack is a powerful set of APIs, all enabled by Aadhaar authentication. As described on the India Stack website:

> **"India Stack is a set of APIs that allows governments, businesses, startups and developers to utilise a unique digital Infrastructure to solve India's hard problems towards presence-less, paperless, and cashless service delivery."[81]**
>
> India Stack's website

It is a set of APIs operating in "layers" that achieve these goals, a set of tools for developers to produce the apps and services—all linked back to Aadhaar.

Examples of apps that use India Stack can be seen in the "Build on India Stack" competition, run by iSPIRT and various partner organisations, both Indian and international[82]. This is a competition for startups that are making use of India Stack in their products. Winners included fair collection for transport networks, apps that offered credit to farmers, and saving and lending apps[83].

Who is building India Stack, this set of APIs? It is being produced, ostensibly, by "volunteers", operated by iSPIRT (the India Software Product Industry Round Table) —a high-powered think tank. Having India Stack as a product produced by a group of 'volunteers'—rather than, say, within the the UIDAI (Unique Identification Authority of India)—has certain advantages from their point of view: they do not have to operate

[78] India Stack presentation" available from http://www.slideshare.net/ProductNation/india-stack-towards-presenceless-paperless-and-cashless-service-delivery-an-ispirt-initiative

[79] iSpirt website: http://www.ispirt.in

[80] "Lenddo Score API Docs", Lenddo website, https://www.lenddo.com/documentation/rest_api.html Accenture (2017) "PSD2: How Can Banks Seize The Opportunities", https://www.accenture.com/gb-en/insight-psd2-opportunities-banks

[81] "What is India Stack?", India Stack website, http://indiastack.org/about/

[82] "Build on India Stack Venture Pitch Competition", Build on India Stack website, http://www.buildonindiastack.in

[83] "Build on India Stack Venture Pitch Competition", Build on India Stack website, http://www.buildonindiastack.in

transparently, there is no requirement for them to be subject to right to information legislation or procurement rules. Thus, this important initiative—potentially as important as anything coming from government ministries—is not subject to that degree of oversight.

At the heart of this innovation lies peoples' data: not just payment and commerce data, not just the data from the layers in the stack, but also social data, the data from the interactions that Indians make and the lives that they're living. As Nandan Nilekani, former chairman of the UIDAI (Unique Identification Authority of India), wrote, the power of India Stack will be to "enable consumers and business to harness the power of their own data to get fast, convenient and affordable credit. Such use of digital footprints will bring millions of consumers and small businesses (who are in the informal sector) to join the formal economy to avail of affordable and reliable credit. And as data becomes the new currency, financial institutions will be willing to forego transaction fees to get rich digital information on their customers."[84]

Looking at some of the key elements of India Stack illustrates how this initiative, built upon Aadhaar, operates in some concerning areas. The focus of this discussion will be on two layers of India Stack that are particularly problematic in the field of fintech: eKYC and UPI.

eKYC

One of the layers of India Stack is the eKYC (electronic know your customer) layer. This is designed for uses like presence-less bank account opening. It has, however, resulted in a change to the operation of Aadhaar that puts the privacy of Indians at risk, a change to the nature and risks associated with Aadhaar as well as indicative of how changes to the operation of Aadhaar in the future can create new risks.

Under its initial implementation, the centralised database of Aadhaar had a single purpose, answering a single yes/no question: do the biometrics of this person match those stored for their Aadhaar number? So, when someone is seeking to authenticate their identity using Aadhaar, they do so either with their biometrics (either a fingerprint or an iris scan) or through a one-time pin (OTP) sent to their registered mobile number. This is checked against the data held in the Central Identities Data Repository (CIDR) database, and the reply is done on a "yes/no" basis: an individual's Aadhaar number, and their biometric data or a OTP, is transmitted to the CIDR database, and an answer of only "yes/no" is returned[85].

This is how the system stood under the National Identification Authority of India Bill 2010 (NIAI), under which no additional data from the CIDR could be returned: "The Authority shall respond to an authentication query with a positive or negative response or with any other appropriate response excluding any demographic

[84] Nilekani, N. (2016) "Forward" in Credit Suisse "India Financials Sector", https://research-doc.credit-suisse.com/docView?language=ENG&format=PDF&document_id=1062747711&source_id=emcsplus&serialid=Wm0zJuKszkmbCwRYV7hD9c7T64WOziu3Z51RrM7Zcs0%3D

[85] "Aadhaar authentication", UIDAI website https://uidai.gov.in/authentication/authentication-overview.html

information and biometric information."[86] However, this version of the legislation failed to pass both houses of the Indian parliament, and did not become law[87].

Legislation providing for Aadhaar was reintroduced in 2016, as the Aadhaar (Targeted Delivery of Financial and other Subsidies, benefits and services) Bill. This was not passed as a conventional piece of legislation, but was rather pushed through as a money bill[88]. A money bill, as defined in the constitution, has a limited range of provisions related to issues including taxation and the financial obligations of the government; money bills only have to be passed in the lower house. The decision to pass the Aadhaar bill in this form was controversial[89]. Rather than simply being the yes/no response originally proposed for Aadhaar, this Act allows: "any other appropriate response sharing such identity information excluding any core biometric information."[90]

Thus, the nature of the Aadhaar system—and thus the relationship of people with the CIDR database—has changed, with a questionable amount of democratic transparency. This has facilitated an increase in the use of Aadhaar in the financial sphere, as well as elsewhere. For example, the matrimonial site, Love Vivah, advertises itself as "India's 1st matrimonial platform linked with Aadhaar", and requires Aadhaar verification (most likely through a OTP) to register an account[91]. They claim to check the information provided during registration against the UIDAI database, which suggests that they also make use of eKYC.

UPI

Another layer of India Stack is the Unified Payment Interface (UPI). The UPI is a project of the National Payments Corporation of India (NPCI), an umbrella organisation of banks headed by the central bank, the Reserve Bank of India (RBI)[92]. The UPI, essentially, allows apps to transfer funds between a customers' account and another account. This allows funds to be sent to a mobile number, an Aadhaar number, or potentially a virtual address[93], quickly and easily with a simple interface.

Most importantly, this is a set of APIs: this means that the app used by the customer does not necessarily have to use their own bank's app[94]. In December 2016, the Prime Minister launched the flagship UPI app, BHIM. The name BHIM—being an acronym

[86] "Hello Aadhaar, Goodbye Privacy", The Wire, 24th March 2017, https://thewire.in/118655/hello-aadhaar-goodbye-privacy/

[87] "The Rights and Wrongs of Aadhaar as a Money Bill", The Wire, 7th March 2016 https://thewire.in/24115/arun-jaitley-introduces-money-bill-on-aadhar-in-lok-sabha/

[88] "Aadhaar legislation tabled as a money Bill", The Hindu Business Line, 3rd March 2016, http://www.thehindubusinessline.com/economy/new-aadhaar-bill-introduced-as-money-bill-in-lok-sabha/article8309587.ece

[89] "The Aadhaar Act is Not a Money Bill", CIS India, https://cis-india.org/internet-governance/blog/the-aadhaar-act-is-not-a-money-bill

[90] "The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Bill, 2016", Bill No. 47-C of 2016, Passed on 11th March 2016 http://www.prsindia.org/uploads/media/AADHAAR/Aadhaar%20bill%20as%20passed%20by%20LS.pdf

[91] Love Vivah website, https://www.lovevivah.com

[92] NPCI website, https://www.npci.org.in

[93] NPCI "Unified Payment Interface API Technology Specification v.1.21", previously available at http://www.npci.org.in/documents/Unified_Payment_Interface_API_Technology_Specifications%20_v121.pdf

[94] NPCI "Unified Payment Interface API Technology Specification v.1.21", previously available at http://www.npci.org.in/documents/Unified_Payment_Interface_API_Technology_Specifications%20_v121.pdf

standing for “Bharat Interface for Money”—was explicitly chosen as a reference to Dr Bhim Rao Ambedkar, the ‘father of the Indian constitution’[95]. Thus it develops a nationalist rhetoric that is running throughout the Indian fintech sector. Again, Prime Minister Modi played up the themes that developed during the demonetisation period, announcing at the launch: “BHIM-App’s success will be a global case study in coming days. It’s a unique concept in the field of financial sector across the world where such app will neutralise black money and corruption.”[96]

UPI is spreading. It was reported in April 2017 that WhatsApp was looking to use UPI in its app for transferring payments[97]. UPI is also being used for payment for Uber[98] and within the popular payment app PayTM[99].

It is true that UPI allows for some limitation in information disclosure, i.e. individuals don’t need to share bank account data with one another, but it nonetheless vastly increases the amount of data generated, and from there, the potential for additional processing. The Chief Operating Office of NPCI, Dilip Asbe, described the goal of the UPI as “unlocking [the customers’] data footprint via data APIs”[100]. The NPCI sees the data produced by the UPI as an opportunity for banks to understand more about their customers, as well as to develop credit histories to be used for lending. In terms of the relationship between the public and the providers of financial services, this provides a shift: increased power, and the collection of more data about the transactions of Indians.

[95] “PM Narendra Modi launches UPI based mobile payment app called BHIM”, The Economic Times, 31st December 2016, http://economictimes.indiatimes.com/news/economy/policy/pm-narendra-modi-launches-bhim-app/articleshow/56254333.cms\

[96] “PM Modi launches Aadhaar-linked BHIM App on Ambedkar’s birth anniversary”, Hindustan Times, 6th May 2017 http://www.hindustantimes.com/india-news/pm-modi-launches-aadhaar-linked-bhim-app-on-ambedkar-s-birth-anniversary/story-JwXr62Wwx7ZIgYKkhAognI.html

[97] “WhatsApp picks UPI for payments”, The Ken, 4th April 2017, https://the-ken.com/whatsapp-upi-payments/ (paywall)

[98] “Uber integrates with UPI BHIM payment for riders”, Economic Times, 23rd August 2017 http://economictimes.indiatimes.com/small-biz/startups/uber-integrates-with-upi-bhim-payment-for-riders/articleshow/60194663.cms

[99] http://www.livemint.com/Industry/pkRT1hq7pyn2RIUvgB95aN/Paytm-Payments-Bank-to-launch-UPIbased-service.html

[100] Public seminar with Dilip Asbe, Chief Operating Officer (COO) of National Payments Corporation of India (NPCI), NIPFP, New Delhi, November 16, 2016. Attended by author.

Part 3: The Growing Scope of Financial Identity

There has been a massive growth in the amount and nature of the data that is gathered by financial institutions about individuals. Many new data sources feed into the creation of financial identities. This is particularly visible through an exploration of the increase in the scope of credit scoring, a context in which these financial identities are used to make judgements about people.

Data and Credit Scoring

Credit scoring is defined by Raymond Anderson as[101]:

> **"the use of statistical models to transform relevant data into numerical measures that guide credit decisions. It is the industrialisation of trust; a logical future development of the subjective credit ratings first provided by nineteenth century credit bureaux, that has been driven by a need for objective, fast and consistent decisions, and made possible by advances in technology".**

India Stack's website

Prior to the 1960s, much lending was primarily based on the personal knowledge of each other (for example, between a local branch bank manager and the customer). However, with the increase in the volume of people seeking credit, and its availability, this meant that this was no longer practical. Thus, this fostered the emergence of other, allegedly objective, ways of offering credit.

The alleged objectivity of credit scoring also has the purported consequence of preventing discrimination that was seen to be introduced by offering lending based on personal interactions: "This objectivity helps lenders ensure they are applying the same underwriting criteria to all borrowers regardless of race, gender, or other factors prohibited by law from being used in credit decisions."[102] It can be questioned as to whether this was ever actually achieved. As more of these credit decisions are made by algorithms, the issues of discrimination only rise[103].

[101] Anderson, R. (2007) The Credit Scoring Toolkit, OUP, page 6

[102] Mester, L. (1997) "What is the point of credit scoring?" in Business Review (Federal Reserve Bank of Philadelphia, page 8 https://www.researchgate.net/profile/Loretta_Mester/publication/5051659_What_Is_the_Point_of_Credit_Scoring/links/54b668cf0cf2bd04be32098a.pdf

[103] See case studies of discrimination and algorithms at: https://medium.com/@privacyint/invisible-manipulation-efb4243011ca

There is an increased move to make aspects of it more transparent and communicated to the individual[104]. However, there is a tension, Mark Kear argues, between the dual role of credit scoring: between its role as an evaluator of financial behaviour and its role in the modification of financial behaviour[105]. This is the problem that leads individuals to "game the system", if they understand how internal workings of credit decision-making works. This is a tension that has not been resolved by the credit scorers discussed below.

"Alternative Credit Scoring"

There has been a vast increase in the scope of the data that is potentially used by some credit scorers. The needs of "thin-file" or "no-file" customers have been a group that credit scorers have focused on for a while; for example, in 2004, the US agency FICO introduced a score for this group, making use of data from utility and rental companies, payday lenders, and other sources that had previously not played into their scoring[106]. However, the use of the sources of data has increased spectacularly. Given that this sector targets those without an existing credit history, this means that most of the potential market is amongst the poorest and most vulnerable in society.

"All data is credit data"[107]—as the CEO of Zest Finance and former Google CIO Douglas Merill famously said. Data that would have been considered irrelevant —or even absurd—to determining an individual's credit risk is now leveraged for credit scoring: as the examples below show, how we arrange our phone's contacts or even how often we call our relatives can become a factor in credit scoring.

M-Pesa in Kenya

The mobile money transfer service M-Pesa was launched by Safaricom in Kenya in 2007. It has proven massively popular, with 237 million person-to-person transactions taking place in 2013[108]. With the service reaching its tenth birthday, Safaricom stated that M-Pesa has generated more than US$1 billion, and generated 860,000 jobs[109]; whether this account is accurate or not, the near-ubiquity of M-Pesa is undeniable, as are the social changes that it has brought[110].

[104] Mazer, R. (2017) "Digital Credit: Data Sharing Can Improve Product Diversity", CGAP http://www.cgap.org/blog/digital-credit-data-sharing-can-improve-product-diversity

[105] Kear, M. (2014) "The scale effects of financialization: The Fair Credit Reporting Act and the production of financial space and subjects in Geoforum volume 57 http://www.sciencedirect.com/science/article/pii/S0016718514001821

[106] Anderson, R. (2007) The Credit Scoring Toolkit, OUP, page 258

[107] "Facebook Isn't So Good at Judging Your Credit After All", Wall Street Journal, 24th February 2016 https://www.wsj.com/articles/lenders-drop-plans-to-judge-you-by-your-facebook-friends-1456309801

[108] "M-Pesa And The Rise Of The Global Mobile Money Market", Forbes, 12th August 2015 https://www.forbes.com/sites/danielrunde/2015/08/12/m-pesa-and-the-rise-of-the-global-mobile-money-market/#21682f325aec

[109] "Safaricom's CEO: A decade on, M-Pesa has room to grow", Africa Report, 3rd March 2017, http://www.theafricareport.com/East-Horn-Africa/safaricoms-ceo-a-decade-on-m-pesa-has-room-to-grow.html

[110] For example, as far back as 2009, social changes brought by M-Pesa had been noted. See Morawczynski, O. and Pickens, M. "Poor People Using Mobile Financial Services: Observations on Customer Usage and Impact from M-PESA", CGAP Brief, https://www.cgap.org/sites/default/files/CGAP-Brief-Poor-People-Using-Mobile-Financial-Services-Observations-on-Customer-Usage-and-Impact-from-M-PESA-Aug-2009.pdf

Yet a change that has not been much explored is that M-Pesa also produces a vast amount of data for the telco Safaricom. Each of the millions of transactions that take place a year tell a story. They tell the story of how the small business is operating: the money they are sending to their suppliers, the transactions that are taking place. But it tells other stories as well: the money that comes in and then is sent to the hospital. The school fees paid by the biological father, unknown to anyone except the mother, father and Safaricom.

But there is also a way in which this data is known by third parties. The transmission of the content of the money transfers over M-Pesa is encrypted. However, the details of any transactions are sent, unencrypted, by plain SMS. Even if M-Pesa transactions themselves are sent via secure and encrypted means, the account information is not. The messages that someone sends for receiving or sending money include the name of the recipient (from the registration of the SIM), the amount sent, and their current balance. This facilitates the gathering of personal data by apps.

The fact that the transactions can be tracked becomes a large part of the power of the lenders, as in the Kenyan example, leaving a trail via the M-Pesa SMS messages for both customer and retailer. As shall be illustrated, this is an aspect of M-Pesa of which fintechs are able to take advantage.

Three Companies

The following section explores the themes emerging from three fintech companies.

1. Tala: Tala was founded by the current CEO, Shivani Siroya. Headquartered in Santa Monica, California, it offers loans in countries including Kenya and the Philippines. The data scientists who analyse this data are based in California, and customer data is also held in the US. All of the algorithms, for Tala's operations all over the world, are developed entirely in California.

Tala's founding, as told by their Kenya Country Manager Rose Muturi, is that Siroya saw the smartphones of the most vulnerable: "The beauty is—the information in that can be used for a digitised financial identity."[111] Tala, previously known in Kenya as Mkopo Rahisi, started operating in Kenya in 2014[112].

Tala offers small loans up to US$500 using an app, available on Android via the Google Play store[113]. This app asks for a wide range of permissions, including access to installed apps, contacts, precise location via GPS, the content of SMS messages, and the call log[114]. The Tala app uploads data to Tala's US-based servers every 24 hours, whether the user has even opened the app or not[115]. Customers are encouraged to keep the app on their phone, even if they have been rejected: the app will continue to send their data back to Tala[116]. If there is a change in the model used

[111] Privacy International Privacy International interview with Rose Muturi, Tala, 5th June 2017

[112] Privacy International interview with Rose Muturi, Tala, 5th June 2017

[113] Tala app on Google Play: https://play.google.com/store/apps/details?id=com.inventureaccess.safarirahisi

[114] Tala app on Google Play: https://play.google.com/store/apps/details?id=com.inventureaccess.safarirahisi

[115] Privacy International interview with Rose Muturi, Tala, 5th June 2017

[116] Privacy International interview with Rose Muturi, Tala, 5th June 2017

by Tala to decide who is offered credit, this could mean that people who had formerly been rejected were now offered loans[117].

The app, as it is promoted by Tala, is quick and convenient: it should take 3 minutes to apply for a loan for a new customer, or 1.5 minutes for a returning customer[118]. It saves customers the shame of walking into a bank and being refused a loan, according to Rose Muturi[119].

From the data provided by the app, decisions are made about whether and how people repay their loans. One of the key pieces of data is to analyse the content of SMS messages for the records of M-Pesa payments. These are very valuable records to analyse; for example, if the person seeking a loan has a small business, it is a good measure of the health of the business and the money entering and leaving the business. But, according to Tala, it can also be used to analyse how people are actually using their loans, as frequently the money they receive from Tala will leave someone’s M-Pesa account immediately (for example, to pay school fees or a hospital loan, or an individual)[120].

But the analysis of the data by Tala extends beyond this, to make analyses based on data and information that are, at best, unexpected to be used for credit scoring. For example, Tala analyses call logs: their analysis has found that people who make regular calls to family are 4% more likely to repay their loan. To do this analysis, they need to know who your family is: from the content of text messages that call someone “mama”, and the pattern of calls[121].

2. Branch: Operating along similar lines to Tala, Branch is also a California-based startup with operations in Kenya but looking to expand elsewhere in developing markets. As with Tala, the data scientists at Branch are based in California—in this case, San Francisco.

Branch also offers loans via its app on Google Play[122]. The app asks for a similar set of permissions as Tala; it gains access to permissions including the content of the user’s call log, contacts, SMS messages, and precise location via GPS[123]. As many of the people borrowing are running small businesses, access to the data held in M-Pesa SMSes on a phone is valuable: a small business owner would not necessarily understand what a profit-and-loss statement is, as a Branch employee explained, but Branch can find that information from the M-Pesa SMS messages.

Daniel Szlapak of Branch was straightforward with the trade-off that was being made: “Are they willing to trade privacy for uncollateralised credit? Without a doubt.” [124] But

[117] Privacy International interview with Rose Muturi, Tala, 5th June 2017

[118] Privacy International interview with Rose Muturi, Tala, 5th June 2017

[119] Privacy International interview with Rose Muturi, Tala, 5th June 2017

[120] Privacy International interview with Rose Muturi, Tala, 5th June 2017

[121] Privacy International interview with Rose Muturi, Tala, 5th June 2017

[122] Branch app on Google Play: https://play.google.com/store/apps/details?id=com.branch_international.branch.branch_demo_android

[123] Branch app on Google Play: https://play.google.com/store/apps/details?id=com.branch_international.branch.branch_demo_android

[124] Privacy International Privacy International interview with Daniel Szlapak, Branch, 6th June 2017

he was clear on the alternative, that people would otherwise go looking for credit at moneylenders. With Branch, "Yes, Big Brother is watching you, but not standing at your door with a stick."[125]

One difference from Tala is that Branch also makes use of Facebook for authentication[126]; as discussed below, this is allowed under Facebook's terms and conditions. Another factor that Branch uses for its decision-making is the behaviour of your friends, and their repayment patterns for Branch loans. How does Branch know who your friends are? They have a refer-a-friend feature (as does Tala), which is one source of this data. But they can also see your Facebook friends, and your call log to know who is contacted regularly[127].

In the future, Branch is looking to expand its operations, beyond lending, including insurance and savings. Daniel Szlapak of Branch is looking towards a future—perhaps 50 years in advance—where credit is free, monetised via other means such as advertising in apps. The avenues of expansion of these types of apps is based on ever-more analysis of the data that they have collected, stored and analysed.

3. M-Kopa: M-Kopa differs from Branch and Tala, in the sense that it does not use a mobile app but rather is a fintech that offers loans for its solar panel system, as well as other goods.

The basic M-Kopa device, the M-Kopa IV Solar Home System, consists of an 8W solar panel which charges a battery, which powers 3 LED light bulbs, a LED torch, a phone charger, and a radio[128]. The customer pays a deposit of 2,999 Kenyan shillings (approximately US$30), and then pays 50 shillings a day (approximately 50 US cents) a day for a year[129]. Payment is via M-Pesa on their mobile phone. While the terms of repayment are 365 days—i.e., 9,125 shillings on top of the deposit—the customer will lose access to electricity but suffer no other direct penalty for not paying the charge for a particular day.

The devices that M-Kopa sells contain a 2G SIM card, the main purpose of which[130] is for billing. According to Chad Larson, one of the founders and current Finance Director, the data transmitted from the device is used for further analysis. Even though a side effect, they are taking advantage of this: they have a team of data scientists based in Nairobi, all Kenyans with Ivy League degrees[131].

After the initial payment for the loan is repaid, M-Kopa may offer borrowers additional products, depending on the pattern of repayment of the initial loan. M-Kopa's "killer app" is the upgraded version of their system, the M-KOPA 400, which has a larger panel and battery to power a 16" digital TV. This version of the system requires a 7,999-shilling deposit (approximately US$78 dollars) and 125 shillings (US$1.20) a day for a year[132].

[125] Privacy International interview with Daniel Szlapak, Branch, 6th June 2017
[126] Privacy International interview with Daniel Szlapak, Branch, 6th June 2017
[127] Privacy International interview with Daniel Szlapak, Branch, 6th June 2017
[128] M-Kopa website: http://www.m-kopa.com/products/
[129] M-Kopa website: http://www.m-kopa.com/products/
[130] Privacy International Privacy International interview with Chad Larson, M-Kopa, 9th June 2017
[131] Privacy International interview with Chad Larson, M-Kopa, 9th June 2017
[132] M-Kopa website: http://www.m-kopa.com/products/

Other customers, who paid their initial loan more slowly, might be offered a cook stove or water tank, for instance[133]. In the future, they may offer other products, but there are regulatory hurdles for offering services like cash loans. In any event, if someone does not pay the daily rate on their water tank or cook stove, their electricity would be cut off.

The data that M-Kopa gathers from the device via the SIM is information like location (using cell data, not GPS), the charge level in the battery, and what devices are plugged in[134]. They will also soon be gathering data on the television programmes watched[135]. This specific data on programming is not data that it is planning to sell, but rather to use to develop its own services in the future[136].

M-Kopa's website states that, "After completing payments, customers own the product outright."[137] However, the customer does not own their data. The terms and conditions of a M-Kopa loan make the company's position on data clear: "M-KOPA shall have absolute and sole ownership of … the data which is obtained by the Customer's use of the Device."[138] Customers have no right to even see their own data, apart from the provisions under Credit Reference Bureau rules[139].

For M-Kopa, it ultimately comes down to a business decision: "If data privacy was important for the Kenyan consumer, we would do it,"[140] states Chad Larson, the Chief Credit Officer at M-Kopa. At the same time, both M-Kopa and its investors have a viewpoint that their use of data is ethical[141].

M-Kopa has a relationship with Safaricom. M-Kopa has become the third largest user of M-Pesa by volume (especially now that fees under 50 shillings have been waived) [142]. They have a deal over the SIM cards in the M-Kopa device, and the data charge on those; this benefits Safaricom as they have found that people who use M-Kopa spend more on their phones, perhaps as they have more spare income or they can be kept charged[143].

Themes Emerging from the Kenya Credit Scoring Examples

There are a number of themes emerging from these examples. The Omidyar Network, in a survey of the consumers of alternative credit scoring services in Kenya and Colombia, asked which data they considered most private. Calls and texts were considered private by 82% of respondents in Kenya and Colombia, above data such as medical and financial data[144]. As the examples in this chapter show, this is amongst

[133] Privacy International interview with Chad Larson, M-Kopa, 9th June 2017
[134] Privacy International interview with Chad Larson, M-Kopa, 9th June 2017
[135] Privacy International interview with Chad Larson, M-Kopa, 9th June 2017
[136] Privacy International interview with Chad Larson, M-Kopa, 9th June 2017
[137] M-Kopa website: http://www.m-kopa.com/products/
[138] Terms and conditions on M-Kopa website: http://www.m-kopa.com/terms/
[139] Privacy International interview with Chad Larson, M-Kopa, 9th June 2017
[140] Privacy International interview with Chad Larson, M-Kopa, 9th June 2017
[141] Privacy International interview with Chad Larson, M-Kopa, 9th June 2017
[142] Privacy International interview with Chad Larson, M-Kopa, 9th June 2017
[143] Privacy International interview with Chad Larson, M-Kopa, 9th June 2017
[144] Costa, A., Deb, A., and Kubzansky, M. (2016) "Big Data, Small Credit: The Digital Revolution and Its Impact on Emerging Market Consumers" Omidyar Network, page 20-21 https://www.omidyar.com/sites/default/files/file_archive/insights/Big%20Data,%20Small%20Credit%20Report%202015/BDSC_Digital%20Final_RV.pdf Omidyar

the key data sources used for alternative credit scoring in Kenya. This data is being used by lenders like Tala and Branch, without the protections that might be expected for this data, as illustrated below.

There are also other concerns: the scope of what falls within the concept of financial identity. More and more aspects of people's lives are falling within the scope of what that is; more is being observed, analysed, and affecting an individual's financial standing. Along with that increase in scope comes an increase in power, of fintech companies themselves as well as the financial sector more generally.

"Gaming the System"

Fintechs face the risk that users will "game the system": i.e., that the customer will manipulate the system to achieve the outcome that the customer wants. This becomes particularly problematic when you are in the field of alternative credit scoring, as it results in a change of behaviour away from the usual financial realm, and can enter into issues like how one behaves and who one communicates with.

Tala claims that it is not possible to 'game' their system in this way[145]. Because they collect so many factors and data points, they claim, it is not possible to manipulate the system. However, they claim that some other apps (that they decline to name) did offer the possibility of 'gaming': these are apps with a sophisticated front-end but lacking a sophisticated backend, claims Tala, that are susceptible to manipulation[146].

This account admits that some models employed in fintech could potentially be manipulated, even if no fintech would admit that their own system could be manipulated. Further, it does not quite address the issue, if the concern is that fintech will change behaviour. It is as important that people have beliefs that result in a behaviour change than whether such beliefs are accurate. The latter impacts an individual's score, and the bottom line of the fintechs, whereas the former affects society more broadly.

Control Over the Data

A significant issue with the fintech companies in Kenya is that they keep access to the data. They keep the data—and, in some cases analyse it, even if the user has stopped being a customer of theirs, and has deleted their app. Branch is explicit that it keeps the data even after a user uninstalls the app, and admits it is possibly doing further analysis on it, "we have that right."[147] Tala encourages people, even if they have been rejected for a loan, to keep the app; if they do delete it, Tala retains their data. This is so that, if the customer returns later, they can reinstall the app, go through some simple KYC checks, and be able to borrow again[148]. M-Kopa, on the other hand, continues to collect data from the device even after the loan has been repaid[149].

[145] Privacy International interview with Rose Muturi, Tala, 5th June 2017
[146] Privacy International interview with Rose Muturi, Tala, 5th June 2017
[147] Privacy International interview with Daniel Szlapak, Branch, 6th June 2017
[148] Privacy International interview with Rose Muturi, Tala, 5th June 2017
[149] Privacy International interview with Chad Larson, M-Kopa, 9th June 2017

Another problem is that much of the fintech startup capital is funded by venture capital; this means that startups are looking for an exit strategy, often within 6-8 years[150]. In many cases, this will be that the fintech is sold. As the Branch privacy policy makes explicit, "We may disclose your personal information to third parties… if Branch International or substantially all of its assets are acquired by a third party, in which case personal data held by it about its customers will be one of the transferred assets."[151] Similarly, in an interview, Chad Larson of M-Kopa stated that the goal was eventually to sell the company—and, in doing so, "future scenarios exist where they are not in control of that data"[152].

This does not paint a rosy future for the protection of personal data in the fintech space. Given that the goal of fintech startups is to be sold, if the fintech space continues to be a commercially viable one then the consequence of this will be the consolidation of the market. At the very least, the industry's business model is designed with the consequence that its customers do not know, in the future, who will have control over their data or what safeguards will be put in place.

Deconstructing "Trust"

Tala's founder writes in a blog post on the importance of trust: "Our credit scores, or what we like to call financial identities, help our customers become visible and trusted— thereby putting power in their hands."[153] But, in a crucial respect, this trust only goes in one direction. Customers are required to trust Tala with their data, but Tala's trust only goes along with data and knowledge. There are ways that they do not trust their customers: for example, they do not ask about whether a business is registered because the only way to check this would be to do it manually, which they are not able to do; so they do not ask the question[154]. They do not show meaningful trust towards the customers acting honestly, they require evidence.

Social Media and Fintech

The use of social media for credit scoring is a popular topic for media; for example, the Financial Times reported that saying that you get drunk on Facebook would impact upon your credit score[155]. The US credit scorer FICO was quick to state that, while posts about being 'wasted' on Facebook could be predictive of a customer's ability to repay a loan, FICO was not using such data in its scoring decisions[156].

While noting that "All data is credit data", Douglas Merrill, CEO of Zest Finance added:

[150] "Venture Capital with a Twist: How to Pitch an Impact Investor", Omidyar Network webpage, https://www.omidyar.com/blog/venture-capital-twist-how-pitch-impact-investor

[151] Branch privacy policy https://branch.co/pp

[152] Privacy International interview with Chad Larson, M-Kopa, 9th June 2017

[153] Siroya, S. (2017) "The Future of Finance Starts with Trust", https://medium.com/tala/the-future-of-finance-starts-with-trust-bfa79f05893a

[154] Privacy International interview with Rose Muturi, Tala, 5th June 2017

[155] "Being 'wasted' on Facebook may damage your credit score", Financial Times, 15th October 2015, https://www.ft.com/content/d6daedee-706a-11e5-9b9e-690fdae72044

[156] "Being wasted on Facebook won't hurt your credit score – at least not yet", GeekWire, 30th October 2015 https://www.geekwire.com/2015/being-wasted-on-facebook-wont-hurt-your-credit-score-at-least-not-yet/

"We've determined it's creepy to use social media."[157] Fintechs, however, do make use of aspects of social media. A pioneer in this space was Lenddo, who in its early years made extensive use of social media for credit scoring[158].

An example of the changing attitudes towards social media data is that of the British company Big Data Scoring (BDS). Writing in 2013, the founder and CEO Erki Kert[159] stated:

> **"Once our plug-in is added to your on-line loan application, we collect the following data for your clients from Facebook:**
>
> **Complete user profile and activity information (including basic data (such as education, relationship status, workplace, number of friends, etc.), likes, groups they belong to, status updates, locations, etc.)**
>
> **A selection of information on the applicant's friends (education, workplace, etc.)**
>
> **All in all, that is c.a. 5,000-10,000 lines of data for each client. From an applicant's point of view, allowing access to all of this Facebook data costs just 2 mouse clicks.**
>
> **The digital footprint of each applicant has strong predictive powers when it comes to determining their credit behaviour. For a lender, it's like having a week to get to know the client properly. We often know more about borrowers than their family or relatives do."**

Erki Kert, BDS CEO

By 2014, they were ready to announce that Facebook data was accurate enough to be the sole source of credit information for loan providers: "We have proven that Facebook can now be your only source of credit information. No need for lengthy loan applications or expensive credit data any more—Facebook and other digital data can be your only source of credit information from here on."[160] They also provided a statistical analysis to back their claims[161], although they did not provide access to the data that they used to reach this conclusion, and there was motive for them to highlight this result in order to promote their product.

[157] "Facebook Isn't So Good at Judging Your Credit After All", Wall Street Journal, 24th February 2016 https://www.wsj.com/articles/lenders-drop-plans-to-judge-you-by-your-facebook-friends-1456309801

[158] "How to get a loan without leaving Facebook", Wired, 15th May 2014 https://www.wired.com/2014/05/lenddo-facebook/

[159] "How we do it", Big Data Scoring website, http://bigdatascoring.com/how-we-do-it/

[160] "Facebook can now be your only source of credit information", Big Data Scoring website, http://bigdatascoring.com/another-breakthrough-in-social-media-credit-scoring/

[161] "Study of credit scoring using only Facebook data", Big Data Scoring website, http://bigdatascoring.com/study-of-credit-scorecard-using-only-facebook-data-3/

By 2017, the position of Big Data Scoring had changed significantly. In May 2017, they produced a piece with the title "Social Media data not suitable for credit scoring"[162], where they stated:

"As time passed and Facebook realized the size and value of the gold mine they are sitting on, they started to limit access to its user data and obtaining valuable information from the social network became more and more difficult.… the way users managed their permissions changed, meaning that people became more aware of the amount and contents of the data they were sharing (a good development in our opinion as we are very much pro transparency and informed behavior)."[163]

Most importantly, however, Facebook changed its platform policy, introducing the prohibition on using Facebook data for scoring. "This made it virtually impossible for any respectable lender to even consider using Facebook data in credit scoring."[164] Big Data Scoring was quick to reassure clients, however, that there is more data than ever available about people: "There is so much more data out there these days about every individual on the planet that is both legally and technically accessible… the scorecards we build on other data sources nowadays are even stronger than the ones based on Facebook data in the first place."[165]

There are still ways in which social media is used by fintechs, beyond Facebook and encompassing other social networking. Tala, for instance uses the number of connections that an individual has, but according to Tala this has less weight than certain other factors related to social media, such as the number of social media apps that a person has on their phone[166]. The length of time that a person spends on social media is taken into account, but could be used to indicate different issues: either the person is unemployed or otherwise has too much time on their hands, or they are running a social-media based business[167].

Social media usage—as with all data points about a user—is not a straightforward statement about an individual's circumstances, rather it is usually only indicative of something. Branch uses Facebook for authentication, which is permitted by Facebook's rules. They use the photo from the Facebook profile to compare with the Kenyan state's Integrated Population Registration System. At the moment they do this manually, although it's possible they'll automate it via facial recognition software in the future[168]. It remains clear that social media will retain a salience in the fintech ecosystem.

[162] http://bigdatascoring.com/social-media-data-not-suitable-for-credit-scoring/

[163] "Social media not suitable for credit scoring", Big Data Scoring website, http://bigdatascoring.com/social-media-data-not-suitable-for-credit-scoring/

[164] "Social media not suitable for credit scoring", Big Data Scoring website, http://bigdatascoring.com/social-media-data-not-suitable-for-credit-scoring/

[165] "Social media not suitable for credit scoring", Big Data Scoring website, http://bigdatascoring.com/social-media-data-not-suitable-for-credit-scoring/

[166] Privacy International interview with Rose Muturi, Tala, 5th June 2017

[167] Privacy International interview with Rose Muturi, Tala, 5th June 2017

[168] Privacy International interview with Daniel Szlapak, Branch, 6th June 2017

Consent

Within the fintech sector—within India Stack as well as the Kenyan apps explored in this report—a great weight is put on the principle of consent. It is the consent layer of India Stack that provides much of its justification, and it is the agreement to accept Android permissions in the case of the apps. However, this weight placed on consent risks weakening the agency and dignity of individuals.

First, consent cannot be seen as a panacea if opting out excludes someone from society. As the MasterCard privacy statement puts it: You can choose not to provide personal information to MasterCard by refraining from conducting payment transactions."[169] Particularly for those who have limited access to financial services, if the only option to accessing services is to agree, consent has limited validity.

Second, there is the question as to whether individuals are able to read and understand the full amount of information required for them to give *informed* consent. There is an extent to which essential information about how an app or service operates is simply not available in any form to the user. For example, an app's permissions do not have to make clear how often or in what circumstances they access a user's data, problematic in the case of the daily uploads from Tala. Added to this is the difficulty involved if a company does not provide their privacy policy in a language understood by the user.

Thirdly, one of the goals of the sector is to change the behaviour of individuals. The 'nudge' is considered a powerful tool in the financial industry: as the academic Sally Brooks argues, we are in a context where behavioural change is the goal of financial services, from the World Bank and elsewhere, often via 'nudge'[170]. But this creates a challenge for the notion of consent. It is an issue that has been discussed within the medical context: "The problem is the potential manipulation of individual decision making through exploitation of rationality: If our choices are manipulated, then this will undermine autonomy and render informed consent out of reach"[171]. In the context of the fintech industry, it becomes troubling to justify so much using the principle of consent, when that consent is being manipulated by the very apps that an individual is using.

[169] "Mastercard - Global Privacy Notice", Mastercard website, https://www.mastercard.us/en-us/about-mastercard/what-we-do/privacy.html

[170] Brooks, S. (2016) "Inducing food insecurity: financialisation and development in the post-2015 era", in Third World Quarterly, volume 37 issue 5 http://www.tandfonline.com/doi/abs/10.1080/01436597.2015.1110014?journalCode=ctwq20are

[171] Brooks, T. (2013) "Should we nudge informed consent?" in The American Journal of Bioethics, volume 13 issue 6 http://www.tandfonline.com/doi/abs/10.1080/15265161.2013.781710?journalCode=uajb20

Conclusion: The Future of Fintech

What future do we want to build for the fintech sector, and how should financial services develop? Unless we look to change course in this sector, the risks and dangers to privacy loom large:

More and more sources of data are used to analyse you by the financial services industry. Everything from where you spend your money to how you spend your time online is all grist for the mill, as the analysis reveals more and more intelligence for the companies. Your everyday movements and your darkest secrets, revealed from your data, are another data point for the companies. Individuals remain largely unaware that this is happening.

It becomes increasingly difficult—and eventually impossible—to escape this, as companies large and small build it into their decision-making processes. If a person wants access to any financial services, it becomes either impossible or prohibitively expensive not to allow access to the most intimate data about themselves.

Technological developments begin to generate more and more data, largely to feed the seemingly endless desire for data of the financial services industry. Cash is discouraged in increasingly draconian ways; the only alternatives do not protect privacy as they generate more data about where you go, what you buy—and are thus used to form judgements about you, your lifestyle, and even your state of mind.

If our starting point for fintech is one in which the notion that being “data-rich” is inherently desirable, then this is the future that we risk building.

But there can be alternatives. Rather, when we consider the fintech future that we want to build, our starting point should not be that it is acceptable to gather and analyse data about people just because we have the capabilities to do so. Protecting the human right to privacy of people across the globe is an essential consideration.

A Way Forward for Privacy in the Fintech Sector

Challenges Ahead

Our research work on the emerging fintech industry highlights several legal, policy and even ethical challenges for the development of this field.

These challenges include issues such as the leverage and exploitation of social media data, the lack of awareness and control by customers about the data that is collected about them, and a failure by companies to consider socioeconomic contexts.

Much of this is being done outside (or above) laws, policy or ethical considerations, without much oversight of what new problems are being generated as a result. Based on that, we came up with a list of recommendations oriented to different actors in the field:

Recommendations

All actors involved in fintech should take into account the following recommendations:

- Protecting the human right to privacy should be an essential element of fintech. In order to do so, fintech initiatives dealing with personal data should involve comprehensive privacy impacts, taking into account the impact on other human rights such as equality, non-discrimination and economic, social and cultural rights.
- Current privacy regulations should be applicable to fintech, especially international regulations and standards such as the Convention N°108, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and the EU General Data Protection Regulation, without exception. Within this context, clear and rights-respecting cross border data transfer rules are key to ensure a consistent level of protection across countries.
- Customers should be at the centre of fintech, not their product. They should have meaningful access to, and control of, their data, including data mined from the data collected or derived from the profiles that have been generated by third-parties, and information about how it was obtained. Consent should be informed, meaningful, and granular enough to control different possible uses of customer's information. Their data should be used to empower them, not to justify exclusionary practices or surveillance schemes.
- Fintech is not a single technology or business model. Any attempt to implement or regulate fintech should take this diversity into account. In particular, it should be based on the type of activity (i.e., credit scoring) they perform, instead of the type of organisation performing it.

Governments

Governments have a general responsibility to develop and enforce a legal framework to regulate fintech activities. In particular, governments should:

- Develop and implement fintech regulation in a comprehensive manner, coordinating financial, consumer, antitrust, regulatory, cybersecurity, data protection and human rights bodies, guided by best practices and international standards.
- Develop and implement data protection legislation with adequate and coordinated levels of enforcement, addressing the financial sector and regulating cross-border data transfers to ensure equivalent and adequate levels of protection.
- When implementing identity or authentication schemes:
    - carefully assess its need and impacts on privacy and human rights;
    - avoid the creation of new databases or the consolidation of existing ones;
    - make the scheme voluntary, always providing alternative identification mechanisms, not conditioning the provision of any public service upon its use, and providing effective opt-out mechanisms;
    - keeping control of the system and making sure that it works in an open, auditable and secure manner.

Financial and Economic Regulators

National financial and economic regulators should:

- Develop and implement industry standards on the use of new technology-enabled innovations, considering their impact on the financial industry and other sectors.
- Develop and implement guidelines on what data, information and intelligence can be used for decision-making processes across financial services.
- Develop clear and robust standards on the use of profiling and other forms of automated decision making to define strict limitations on when they can be used and ensure that in all circumstances the data subject has the right not to be subjected to a decision based on automated processing without his or her fully informed and explicit consent.
- Regulatory sandboxes are welcomed as long as they do not provide exceptions that undermine fundamental rights such as privacy and personal data protection or increase security risks for that data.
- Regulate and enforce competition rules in financial markets to prevent the formation of data provider monopolies, especially through company acquisition, merger, state privileges, or takeovers.
- Make sure that financial sector companies are liable for mishandling of personal data, both to their clients and also to any other person who could be harmed by industry actors.

- Regulate limitations on data collection for insurance companies, with special emphasis on new tracking devices and technologies.
- Ensure that providers of fintech services are subject to the same data protection and security obligations as traditional financial institutions, and that the international nature of their operations are not being used as a loophole to evade regulation.

Data Protection and Consumer Protection Authorities

Data protection authorities, consumer protection authorities, or their equivalents, should develop guidance on the use of personal data and generated profiles by actors in the financial system including financial institutions, with special consideration to the following:

- Promote and incentivise data minimisation as the best way to avoid the creation of risks for personal data, including the use of technologies that don't involve data intermediaries, like cash or its functional equivalents.
- Restrict the use of this data by government agencies, including law enforcement and intelligence bodies.
- Limit the use or derivation of sensitive data (concerning racial/ethnic origin, political opinions, health or sexual orientation, among others).
- Establish standards for the use of personal data generated by third parties, and in particular internet services providers, for the provision of financial services.
- Develop clear guidelines on the use of profiling and automated decision-making in the design and development of financial services.

On the enforcement side, these authorities should provide oversight over these activities, and investigate the impact of the use of fintech with regards to discrimination and exclusion, with special consideration on its gender impact.

Fintech Industry

The use of personal data for financial services, and the implementation of new decision-making technologies to feed these processes is a challenge that goes beyond mere legal compliance or policy development: it is also an ethical problem. The fact that new systems or technologies can do something does not imply that industry should do it, but requires careful assessment and ethical guidance at all levels.

In the development of innovation in provision of financial services, economic and social considerations should ensure that:

- Any decision-making process regarding the provision of financial services should ensure that only factually accurate data, information and intelligence about the person concerned should be considered.

- There are limits on data collection and the principle of legitimate purpose is respected. Collecting personal data creates important risks for individuals (not only for the customers), so data minimisation (processing only what, and for as long as, is strictly necessary for the legitimate purpose) is a must, not only because of legal obligations, but also because failing to do so will create unnecessary and unforeseen risks.
- In particular, measures should be taken to ensure that profiling and other forms of automated decision-making are subject to very strict limitations and in all circumstances, allow the data subject the right not to be subjected to a decision based on automated processing without his or her fully informed and explicit consent.
- Any person, no matter their relationship with a particular company, must have access to the data, information and intelligence based upon which decisions are made with regards to their ability to access financial services, along with the explanations about how such decisions were made. The access should be enabled in the services by design, be user friendly, and adapted and localised to different contexts, languages and cultural realities.
- Personal data should receive special treatment when assessing its economic value. It is not a commodity and should not be traded as such, given its specific and changing regulatory landscape.
- The security, safety and privacy of the software, hardware and systems used should be guaranteed throughout their lifecycles, protecting personal data from security incidents like data leaks, and from misuse by other groups or governments.

On top of the recommendations outlined above, here are some specific recommendations targeting specific actors within the industry:

- For fintech service providers, they should use customer data only while customers are using their services. Terms of use should not include indefinite amounts of time for data exploitation or background data collection, and should include clear and defined policy effects for circumstances such as customers no longer using a service or uninstalling their apps (not to mention when they delete their profiles).
- For investors, demanding privacy impact and risk assessments from the companies where they have a stake, acknowledging that personal data could become a 'toxic asset' on their portfolio.
- For platforms such as social media companies, monitor and limit the use of their services to build financial profiles, being aware that most information there can be used in that manner, and thus misused.

International Bodies

In addition to complying with relevant legal frameworks, international bodies including international organisations, international financial institutions, international and regional cooperation initiatives, partnerships and task forces as well as philanthropic and grant-making bodies have an ethical responsibility when promoting and funding fintech-related programmes and initiatives to ensure that they promote, respect and protect fundamental rights.

In the development and implementation of these strategies they should:

- Base their research, recommendations, policies and projects regarding financial inclusion and digital identity on inclusive, independent and gender-sensitive research, as well as accurate, relevant and timely data, demanding full disclosure of conflicts of interests from everybody who contributes information to these activities.
- Address the impact of identification and authentication initiatives connected with fintech on privacy and financial exclusion, along with assessing their effectiveness on preventing fraud or money laundering.
- Undertake thorough multi-disciplinary impact assessments of financial inclusion, cashless and digital identity projects they promote or fund, ensuring that they address the needs of individuals and groups at risk of discrimination, vulnerability or marginalisation.
- Include a gender analysis and assessment of the gender impacts.
- Implement mitigation strategies to address unexpected consequences that arise from such projects.

For Other Parties Using Fintech in their Programmes

In addition to complying with relevant legal frameworks, governmental and non-governmental actors whose programmes include fintech-related initiatives have an ethical responsibility to ensure that they promote, respect and protect the fundamental rights of their beneficiaries.

In the development and implementation of these strategies they should ensure that:

- Any decision-making process with the regards to the provision of financial services should ensure that the fundamental rights of the person concerned are respected, and that their data is protected;
- Prior to the deployment of fintech within their programmes and/or projects, in-depth assessments are undertaken:
  - that address the needs of individuals concerned,
  - that include a gender analysis and assessment of the gender impacts,
  - that address the unexpected consequences that arise from the implementation of fintech,
  - that develop mitigation strategies for the risks identified.

~~PRIVACY~~
~~INTERNATIONAL~~

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint

UK Registered Charity No. 1147471