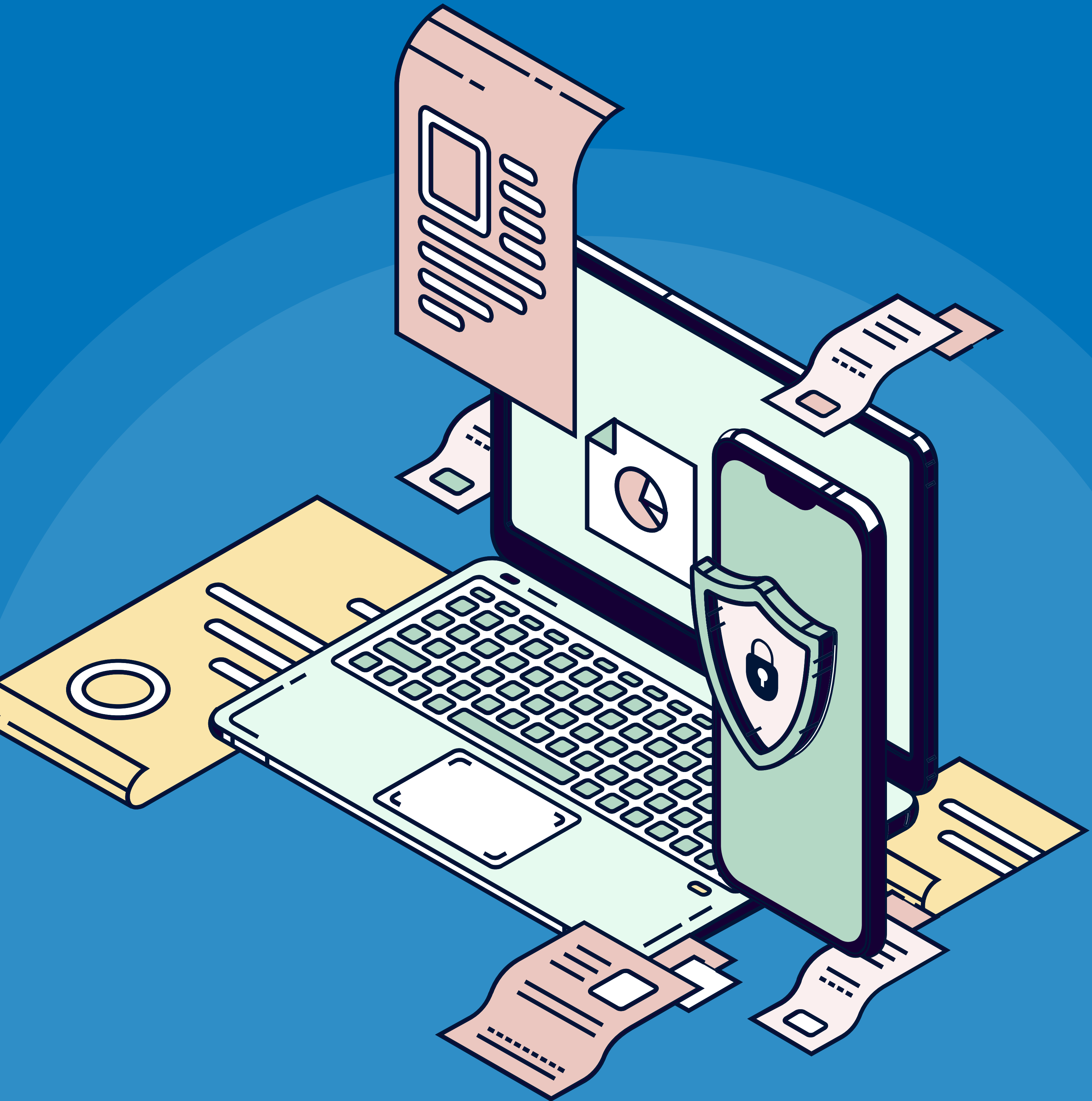
OMIDYAR NETWORK INDIA

Paving the Future

Why PrivacyTech is a rewarding frontier for venture capital

BY SHILPA KUMAR, SUBHASHISH BHADRA AND RAAHIL RAI



About the Authors

Shilpa Kumar is Partner at Omidyar Network India, and provides overall leadership, including strategy and investments, across the areas of Digital Society, Governance and Citizen Engagement, and Property Rights initiatives

Subhashish Bhadra is Principal, Investments, at Omidyar Network India, and works in the Digital Society initiative

Raahil Rai is Associate, Investments, at Omidyar Network India, and works in the Digital Society initiative

About Omidyar Network India

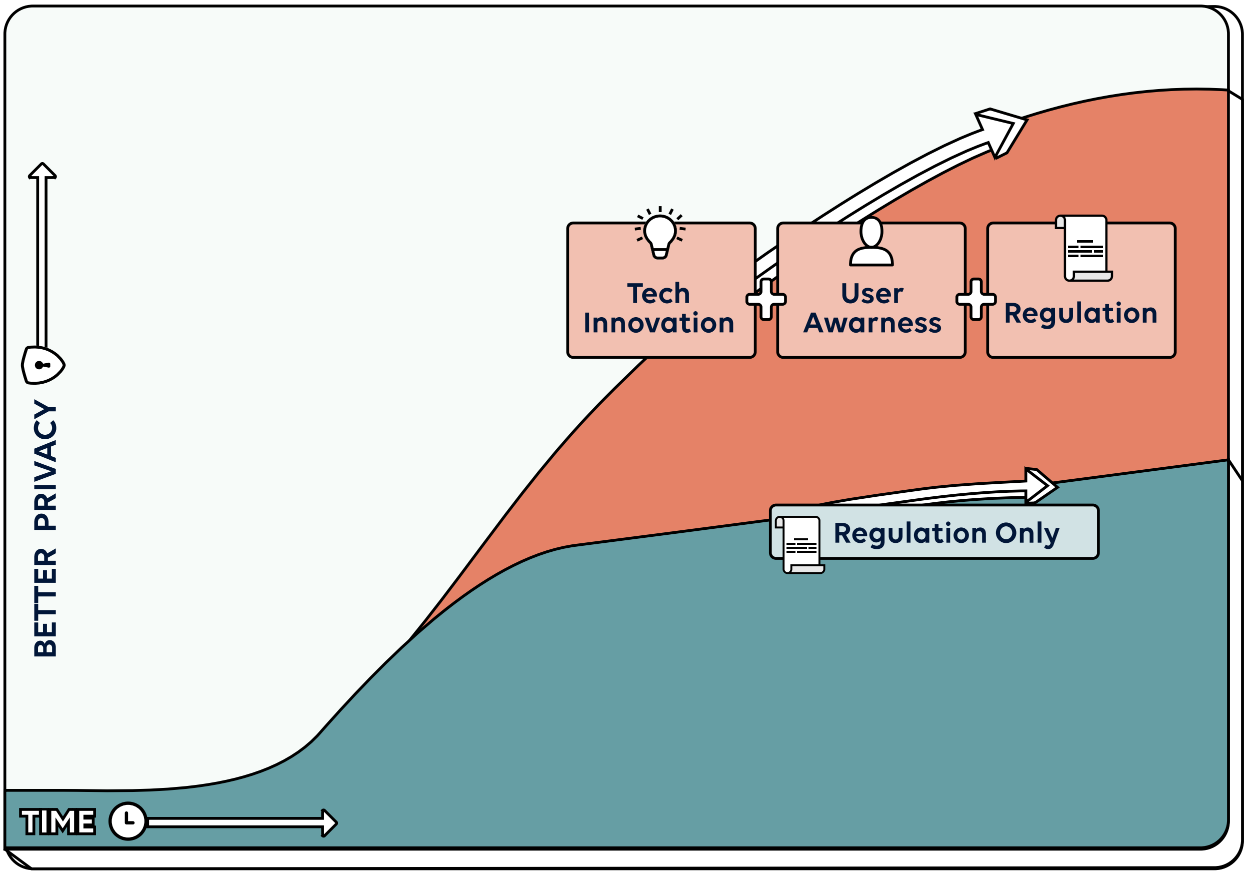
Omidyar Network India invests in bold entrepreneurs who help create a meaningful life for every Indian, especially the hundreds of millions of Indians in low-income and lower-middle-income populations, ranging from the poorest among us to the existing middle class. To drive empowerment and social impact at scale, we work with entrepreneurs in the private, nonprofit and public sectors, who are tackling India's hardest and most chronic problems.

We make equity investments in early stage enterprises and provide grants to nonprofits in the areas of Digital Society, Education, Emerging Tech, Financial Inclusion, Governance & Citizen Engagement and Property Rights. Omidyar Network India is part of The Omidyar Group, a diverse collection of companies, organizations and initiatives, supported by philanthropists Pam and Pierre Omidyar, founder of eBay.

To learn more, visit www.omidyarnetwork.in, and follow us on LinkedIn (Omidyar Network India) and on Twitter (@on_india)

Table of Contents

An Overview



Business Case

- Regulatory compliance
- Rising customer demand
- Increasing investor interest

+

Impact Case

- Digital financial security
- Trust and empowerment online

=

Where We Invest

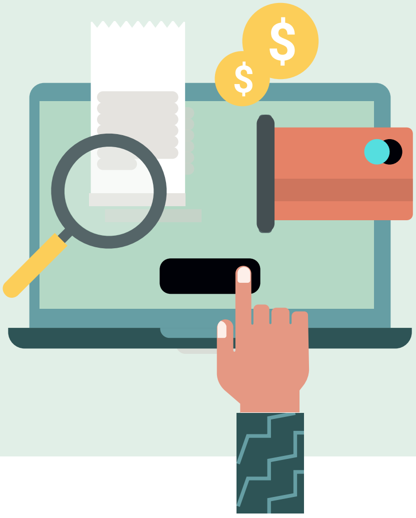
- Data Compliance and Management
- Data Minimisation
- Better Encryption
- Privacy-Forward Consumer Products
- Identity and Access Management
- Identity Verification

Why Privacy Needs Disruptive Tech

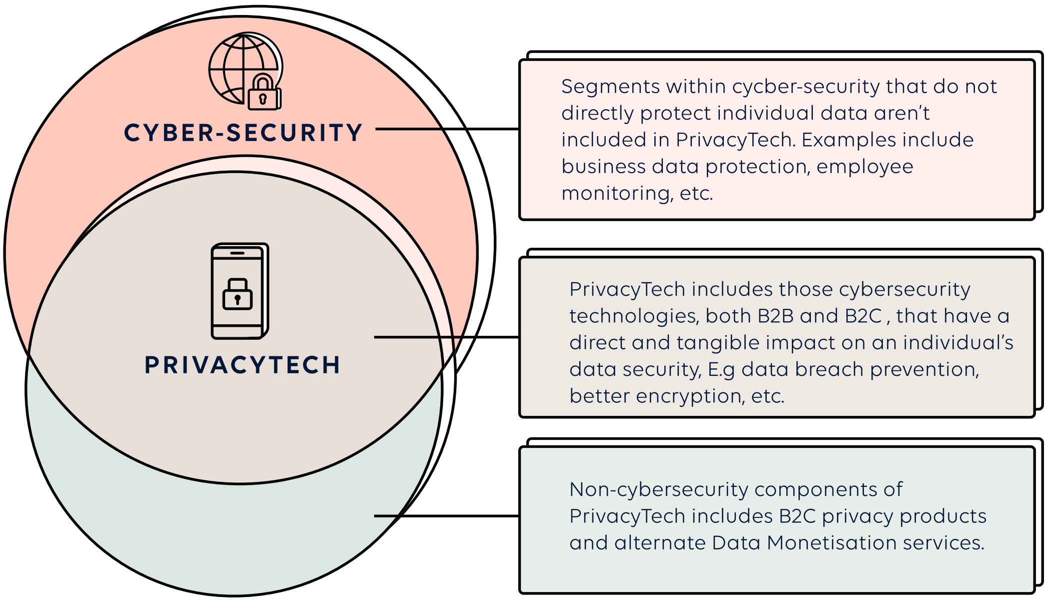
Data was the new oil. Over the last decade, some of the world's most valuable companies were built on refining data. As recently as 2008, only one tech business found a spot among the world's five most valuable companies. Today, the list consists exclusively of tech companies. In the future, data will increasingly become like electricity - more and more businesses will digitize operations to better serve customers- sales, marketing, administration, and customer service- and will, in many cases, morph into being tech businesses, by digitising the product or service itself. Venture capital is flooding into technologies of the future, which will generate still more data. For example, VCs poured $5.1 billion into the IoT sector in the first half of 2020 alone. The data this digitisation generates will underpin all business decisions.

But like oil extraction, data extraction has its own 'inconvenient truth'. Experts have likened data to CO2 - the exhaust from our digital economy that harms us both individually and collectively. Individual awareness of data-based harms is rising, as seen most remarkably in the recent exodus from a popular messaging app that changed its privacy policy. Governments ranging from Europe to California are passing data protection laws that seek to rein in misuse of data.

> "Even if customers wanted to act, and businesses sought to protect them, they lack the technology to make it happen in practice today."



But if customers wanted to act, and businesses sought to protect them, they lack the technology to make it happen in practice today. This leaves customers dissatisfied, businesses vulnerable, and regulators ineffective. Things can change when businesses and individuals adopt technologies and processes that enable them to improve their data practices. We call this nascent sector 'Privacy Tech'. It has significant overlaps with the well-established cyber-security space, but with a greater emphasis on individual control and value.



Segments within cycber-security that do not directly protect individual data aren't included in PrivacyTech. Examples include business data protection, employee monitoring, etc.

PrivacyTech includes those cybersecurity technologies, both B2B and B2C , that have a direct and tangible impact on an individual's data security, E.g data breach prevention, better encryption, etc.

Non-cybersecurity components of PrivacyTech includes B2C privacy products and alternate Data Monetisation services.

In parts of the world where the privacy ecosystem is more mature, venture capital investments have grown substantially over the years, resulting in the emergence of unicorns in the space. Technologies like data breach detection that were once the preserve of large companies, are now becoming mainstream. This growth was driven by an intensifying threat landscape and the European privacy law. Once the Indian law comes into force, we should expect further acceleration. In short, PrivacyTech is set to emerge as an important and rewarding investment area.

Privacy Tech is also important for India's digitisation journey. Between 2017 and 2022, over 500M Indians will have come online for the first time, a group that is called the 'Next Half Billion'. The NHB are low-to-lower-middle income Indians and have very different income profiles, education levels, language skills, and cultural milieus compared to the initial Indian internet users. Many start-ups are using technology to serve the NHB at a lower cost and with better products than before.

However, for the NHB to realise these potential gains, they need to feel empowered and safe online, reap benefits from technology, and face minimal harms from its risks. For this, we need to collectively create a thriving and well-governed digital and data economy. This creates an opportunity for innovators and investors to create the second wave of data businesses - those that responsibly steward consumer data, and minimise risks for data businesses. We hope this document will be useful for venture capital funds, entrepreneurs, and all other stakeholders who seek to create a safe and inclusive digital society for all Indians.

On the Returns Trail

When Europe passed its privacy law in 2016, there were few commercially-attractive Privacy Tech innovations in India - most entrepreneurs were from the US, Europe, and Israel. But India's tech ecosystem has transformed dramatically since then due to the world's cheapest internet access and highest per-capita data consumption. As India becomes an increasingly digital and tech led society, the business case for PrivacyTech is now stronger than ever before.

Regulation has played the most important role - Indian businesses operating overseas need to adhere to privacy laws in Europe, California and elsewhere, and are looking to lower the cost of compliance. All Indian companies may soon need to adhere to a domestic data protection act. In parallel, businesses need to respond to a bottoms-up demand for better privacy from consumers, who are voting with their wallets. Put together, this is drawing in investors, creating a virtuous cycle of innovation and growth.

REGULATION

Since Europe enacted a stringent data protection law in 2016, an increasing number of countries are adopting such laws. India is no outlier - a proposal is pending before Parliament, and may be enacted this year. Such laws impose duties on businesses on how they should handle data, and impose steep fines of up to 4 percent of global turnover for violations.

Regulatory authorities in Europe and elsewhere have already begun to enforce fines. For example, British authorities imposed a $27M fine on British Airways for a data breach, whereas French authorities imposed a $121M fine on Google for failing to obtain consent before placing tracking cookies on users' devices. When India gets a data protection authority, it too will start investigating data practices of businesses.

> Privacy Tech helps businesses reduce the risk and quantum of fines. It also helps them adhere to other obligations under data protection laws in a faster and cheaper way.

Privacy Tech helps businesses reduce the risk and quantum of fines. It does so by reducing the probability of a data breach through better practices, or by helping companies remediate breaches faster. Companies that detect breaches faster can reduce the financial cost of a breach by 25% on average. Privacy Tech also helps businesses adhere to other obligations like data subject rights and data audits in a faster and cheaper way.

Innovation Story

CloudSEK

CloudSEK is a Bangalore-based company that uses an AI-driven digital risk management platform called XVigil to monitor millions of internet sources across the surface web, deep web, and dark web. It detects cyber threats, data leaks, brand infringements, and identify thefts. The actionable insights can be consumed using a SaaS-based dashboard or integrated with existing infrastructure using APIs. CloudSEK's customers include Axis Bank, Kotak Mahindra Bank, IndusInd Bank, NPCI, Gojek, MakeMyTrip among many others.

Logo courtesy: Cloudsek

B CONSUMER DEMAND

Consumers from across the globe are growing wary of trusting businesses offering free tech products. They are migrating to privacy-protecting products and services, which inspire greater trust. When WhatsApp changed its privacy policy in early 2021, its privacy-protecting rival Signal saw downloads increase 4,200%, becoming the most-downloaded app in the world. In just five days, Signal and a similar app called Telegram were downloaded 4.5 million times in India.

When it comes to privacy, consumers are voting with their wallet. A survey of over 2100 Indians from across socio-economic backgrounds found that they are, on average, willing to pay Rs. 32 per month to keep their conversation private. More importantly, behavioral researchers have found that consumers choose products with a better privacy rating.

> “Privacy Tech can help businesses improve their data practices, and use it as a competitive advantage to acquire and retain customers.”

Privacy Tech can help businesses improve their data practices, and use it as a competitive advantage to acquire and retain customers. It can change the consumer-facing interface of businesses in a way that inspires more confidence.

Innovation Story

D-ID
Firewall for your identity.

D-ID is an Israel-based start-up that offers a system designed to protect images from unauthorized automated facial recognition. The product enables images to be processed in a way that causes algorithms to fail to identify the subject through differences that are otherwise undetectable to the human eye. Through this, it facilitates risk-free use of personal data and helps alleviate users' privacy concerns. The company raised a $13.5M Series A in 2020.

Logo courtesy: D-ID

INVESTOR INTEREST

Globally, funders invested close to $10B in privacy and security-related companies in 2019, a five-fold increase from a decade ago. Seed and early-stage deals represented 44 percent of invested dollars. The average deal size increased from $5.1M to $12.14M, representing the entry of larger and later-stage funds.

> Investor interest is leading to higher valuations and profitable exits.

Investor interest is leading to higher valuations and profitable exits. In 2019, US-based threat intelligence firm Recorded Future was acquired at a $780M valuation. Shape Security, a company providing defense against malicious attacks, was acquired at a $1B valuation. Big ID, a data intelligence company that develops software for businesses to satisfy privacy regulations, acquired unicorn status in 2020. The PrivacyTech unicorn club is growing fast.

India is also witnessing increasing interest in such companies. According to a Data Security Council of India (DSCI) report, revenues of Indian cyber-security product firms more than doubled between 2018 and 2020. These companies received nearly $490M of funding from 2017 to 2020, 75 percent of which came from venture capital firms. India has also seen the emergence of unicorns in this space - Druva, a Pune-based Cloud Management start-up, achieved that status in 2019.

Innovation Story

OneTrust
PRIVACY, SECURITY & GOVERNANCE

US-based OneTrust sells a technology platform to help organisations be more trusted, and operationalize privacy, security, data governance, and compliance programs. The integrated platform offers solutions for privacy management, third-party risk, preference & consent management, ethics, compliance, and environmental, social & governance. The product is used by over 7500 customers, including half of the Fortune 500. OneTrust raised a $300M Series C at a $5.1B valuation in December 2020.

Logo courtesy: OneTrust

Impact on Digitising Indians

When Indians go online, they face both visible and invisible risks. Financial frauds have become commonplace, and have made it to public consciousness through shows like Netflix's Jamtara. India tops the global ranking in cyber-bullying of children and in spam email. Misinformation has become chronic on social media, even causing deaths due to social tension or misguided medication.

These risks disproportionately affect India's Next Half Billion because they often lack awareness or recourse. It impedes their digital journey - for example, a survey by the grassroots consumer advocacy group CUTS International shows that Indians will reduce data sharing by 27 percent if their private communication is not encrypted. Behavioral experiments by the Centre for Social and Behaviour Change (CSBC) at Ashoka University and the Busara Centre for Behavioral Economical shows that Indians share 16 percent more data with businesses if they understand the privacy policy better.

Therefore, addressing online risks like privacy can help keep the NHB safe in their digital transition, thus deepening trust and participation in the digital economy. Privacy Tech has a crucial role to play because it enables businesses to be better stewards of customer data, and creates tools that individuals themselves can use to keep themselves safe. Therefore, greater investments in Privacy Tech will help address India's most complex online risks.

In July 2019, Gurugram resident Deepika Gupta received a call from a person claiming to be an employee of a popular mobile wallet app. The caller asked her to complete her KYC application and asked for her debit card details and a one-time password sent on her phone. The caller then disconnected and debited money from her digital wallet. Deepika's story is not unique – every year, thousands of Indians are duped by fraudsters pretending to be banking agents.

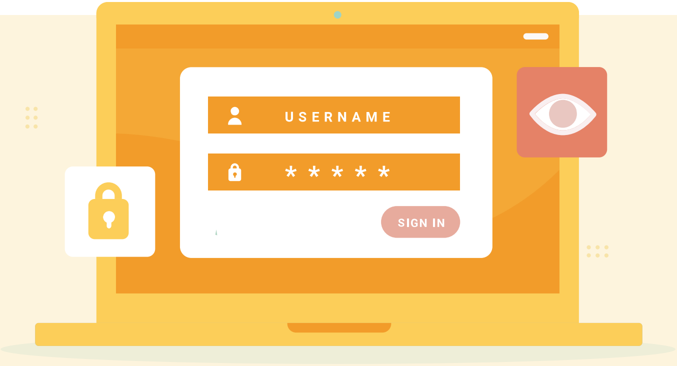
Story courtesy Ribhu Singh of 101Reporters.

DIGITAL FINANCIAL SECURITY

Indians reported 21,000 cases of financial frauds in a single quarter of 2019, resulting in cumulative losses of Rs. 129 crores. The true extent of fraud is likely higher because many do not bother to report it. A 2018 survey found that nearly 18 percent of Indians suffered a financial fraud in the year preceding the survey. Such frauds can be catastrophic for the NHB and wipe away a large portion of their savings.

Financial frauds are intricately linked to poor data practices. Personal data that is leaked by banks or other institutions is used by fraudsters to call the victims, pretending to be a banking agent. Leaked user IDs and passwords can also be used to extract banking information.

Privacy Tech can help banks and other institutions secure their data more effectively. This includes technologies that restrict access to personal data to only those who need to see it, enable quick data breach remediation, or use more secure ways of authenticating the customer's identity. Such technologies will ensure that Indians are less susceptible to online frauds.



> "Such technologies will ensure that Indians are less susceptible to online frauds."

Innovation Story

Hyderabad-based Ensurity provides a passwordless identity and access management solution to businesses. It decentralizes credentials like user name and passwords, so that there is no central honeypot that hackers and others can attack. It has also developed ThinC-Auth, a biometric device used for one-touch access to unlock digital resources both on cloud and on-premises. Ensurity counts Axis Bank, WIPRO, NIC, and HCL among its customers and partners.

Logo courtesy: Ensurity

Nearly 96 percent of Indians with a phone receive spam messages every day. Apart from causing annoyance, these messages also aid financial and non-financial cyber-crimes. 25 percent of Indian internet users aged 13-45 have been subject to revenge porn, most of whom are women. Put together, such incidents create an unpleasant internet experience for the NHB. Consequently, 40 percent of Indians do not trust private or public players with their data.

There are many inter-related reasons for these issues, including commercial harvesting of phone numbers, inadequate content moderation on social media platforms, and lack of recourse for victims. Some issues lend themselves to regulation, whereas others can have innovative tech-based solutions.

> PrivacyTech innovations like spam reduction technologies can help individuals build better online practices that reduce opportunities for abuse.

For example, Privacy Tech can help individuals build better online practices that reduce opportunities for abuse. It can also create tools that help individuals manage multiple identities online. We expect more such innovations to emerge in the coming years.

Innovation Story

DOOSRA

Hyderabad-based Doosra provides its users with a second virtual mobile number that they can share anywhere instead of their actual number, thereby protecting the user's privacy. It addresses the issue that widespread sharing of the mobile number at supermarkets, stores, or restaurants leads to a lot of spam calls and inappropriate messages. Doosra blocks all incoming calls by default, while maintaining call logs and giving the option of identifying trusted contacts and services.

Logo courtesy: Doosra

A Journey Begun

ON India invests in bolds entrepreneurs who help create a meaningful life for every Indian. We focus on the next half billion (NHB), i.e. the 500M Indians who have and will come online for the first time between 2017 and 2022.

Through our Digital Society initiative, we promote the adoption of responsible tech practices such as inclusion, privacy, security, transparency, and good governance. Started in 2016, we have deployed over $13M towards this objective. Our strategy focusses on funding think-tanks and researchers who help India improve its data governance policies, campaigns that work towards informed and active internet users, and stakeholders who build inclusion and safeguards into tech systems. You can read more about the Digital Society initiative's strategy here.

However, these policies and practices alone will be insufficient in the absence of sustainable Privacy Tech business models. Such Privacy Tech entrepreneurs can support the privacy and protection needs of the digitising Indian and enable more privacy conscious and digitally secure businesses. Therefore, ON India is now actively looking for start-ups that support businesses to be more responsible stewards of data, or by enabling individuals to directly take control over their data.

> “ON India is now actively looking for start-ups that support businesses to be more responsible stewards of data, or enable individuals to directly take control over their data.”

OUR INVESTMENT CRITERIA FOR PRIVACYTECH

We believe this sector presents opportunity for both commercial returns and social impact. While investing, we look at-

01

Stage:
We invest in seed, and Series A rounds in companies that have a demonstrated or credible path to monetisation. We lead rounds or come in as co-investors.

02

Amount:
For investments in privacy tech, we invest anywhere between $100K and $1.5M. These amounts may change in the future, as this sector matures.

03

Board Position:
It is important for us to actively contribute to and learn from our equity investments - therefore, we seek a board position - either a member or observer - on most of our portfolio companies.

04

Indian Customer Base:
While we recognise that many of our investments will be B2B and may not serve the NHB today, we seek businesses that that serve a meaningful proportion of Indian customers now or have a clear path to serving them in a five-year time frame.

05

Tech Innovation:
We prefer start-ups that use substantial tech innovation to solve for better privacy, including (but not limited to) deep-tech or category creators that haven't been tested elsewhere globally.

Where We Invest

01

Data Compliance and Management

What it is

Tech products that improve adherence to the obligations under Indian and global data privacy laws. This is a nascent but fast-growing sector globally, and is expected to expand 22 percent annually for the next few years, to reach a $6B global market size by 2025. The Indian market will also grow once the personal data protection bill is enacted.

Opportunity

a. Most existing solutions are services companies, creating space for a productised business
b. Productised business can also reduce cost, creating sales potential in the SMB segment
c. Nuances of local laws may create preference for India-based companies
d. Overseas opportunities in countries that trade heavily with India

Risks

a. Indian market size is uncertain; depends on how active the regulator will be
b. Longer sales cycle because it is a completely new budget head
c. Full productisation may be difficult, because of nuance and subjectivity of regulation, and because Indian companies are habituated to high touch, or assisted model

What We're Looking For

Start-ups offering highly productised solutions that scale non-linearly, and enable businesses to monitor and ensure compliance with privacy laws at low cost.

02

Data Minimisation

What it is

Technologies that enable organisations to carry out existing business processes effectively, while reducing the data footprint. This includes solutions that mask personally identifiable information while customer data is processed by businesses. It also includes new computation techniques that carry out AI algorithms on decentralised data, thus reducing privacy risks. When businesses reduce their data footprint, they are less prone to breaches.

Opportunity

a. Greenfield opportunity, because it is a nascent space even globally

b. Opportunity to innovate and find the right balance between efficiency and privacy

c. Use cases beyond businesses - in academia, government, non-profits, etc.

Risks

a. New budget head for buyers, which results in longer sales cycle

b. Potential loss of speed in business operations

c. Potentially early for Indian market, where other PrivacyTech products take priority

What We're Looking For

Start-ups that have deployed the product with a small cohort of paying customers, and have ideally demonstrated ability to sell in the US and European markets. We will prioritise solutions that result in greater masking of consumer data.

03

Better Encryption

What it is

Technologies that enable businesses to encrypt internal and external communications. The global encryption market is expected to grow at 15.5 percent CAGR, to reach a size of $20B by 2025.

Opportunity

a. Low penetration in India - most data, including those that are breached, are unecrypted

b. Demand for better UI, since more secure forms of encryption today result in greater complexity for users

c. Not a 'winner takes all' market because there are few network effects

d. Quantum computing and other incoming technologies may make older encryption methods obsolete

Risks

a. Necessary but not sufficient product - needs to be accompanied by other technologies

b. Longer sales cycle because it is often a new budget head

c. Lower entry barriers and existing incumbents create commoditisation risk

What We're Looking For

Easy-to-use encryption products that can serve mid-market clients, use more secure techniques like decentralised key management, and are secure against future threats.

04

Privacy-Forward Consumer Products

What it is

Privacy-protecting versions of popular tools and apps. This could include alternative business models that replace data extractivism with trust. Some existing products like Signal are non-profit, whereas those like DuckDuckGo rely on ad revenues. Rising consumer demand will lead to more innovation, and greater experimentation with monetisation models. The market for privacy management tools is expected to grow to $1.9B globally by 2024.

Opportunity

a. Small but fast-growing customer base with demonstrated willingness to value privacy

b. Large information security community in India creates a substantial pool of early adopters

c. Frugal innovation possible, resulting in healthy unit economics

Risks

a. Rate of growth of market size uncertain because privacy is still a niche product

b. Difficult monetisation, because advertising is not a preferred route for privacy businesses

c. Potentially low willingness to pay by Indian customers today

What We're Looking For

B2C Privacy Tech tools that have a clear and short path to profitability, and offer a combined suite of privacy products.

05

Identity and Access Management

What it is

Solutions that enable businesses to limit transactions to genuine customers, thus preventing fraud. For example, banks authenticate users who use net banking and e-commerce platforms authenticate buyers and sellers. It also includes employee controls and access to data inside organisations. IAM is expected to grow at a CAGR of 13% over the next few years, to reach a market size of $25B globally by 2025. Greater digitisation in India is leading to new customer demand.

Opportunity

a. Data breaches are still prevalent and customers are more aware of consequences, Incentivising businesses to secure their perimeter

b. Indian market is currently under-penetrated and relies on OTPs, which are insecure and have been deemed non-compliant by recent EU payments security standards

c. Businesses want to make process seamless and reduce bounce rate substantially

d. Privacy-regulations are leading businesses to gravitate towards technologies that carry out operations without seeing underlying data

Risks

a. Long sales cycle, because products usually require integration with or replacement of legacy systems

b. Large and reputed global competitors, with very little advantage of running an indigenous service

c. High bar on performance, in terms of both accuracy and speed, whereas greater privacy may have a slight impact on performance today

What We're Looking For

Privacy-protecting and zero-knowledge technologies that make online transactions faster and smoother for the NHB.

06

Identity Verification

What it is

Products that help businesses verify the identity and data of new customers, especially those with thin files. Identity verification is a well-established $30B market globally that has large incumbents. However, the nature of the industry is changing fast in a digitising world, creating opportunity for entrepreneurs to disrupt the market.

Opportunity

a. Need for digital solution that serves the NHB at a lower cost

b. Businesses are willing to pay for lower turnaround times and higher accuracy

c. Increasing demand to have privacy-protecting processes because of regulation

d. The NHB is generating more data, creating new ways for them to identify themselves

Risks

a. Existence of large incumbents and lower entry barrier, raising risk of commoditisation

b. Regulation determines whether technologies and processes are permissible for business use, slowing down the adoption of innovative solutions

c. Aadhaar already provides some e-KYC (though limited by court judgments and regulation); innovators will need to show value-add

What We're Looking For

Natively digital technologies that a customer from the NHB can use to identify herself at high speed and accuracy, while preserving the privacy of her data.

ON

OMIDYAR NETWORK INDIA

This whitepaper is for informational purposes only and should not be construed as investment or other professional advice. Information has been obtained from sources believed to be reliable but Omidyar Network and Omidyar Network India do not warrant its completeness or accuracy. Omidyar Network and Omidyar Network India own a significant equity stake in some of the companies referenced in this report, and expect to continue making investments in these and other companies in this sector.