

Driving Data Transformation:

Five Years of Impact
with the IBM Hyper
Protect Accelerator



Table of Contents

Executive Summary	3	Authors
Part 1	4	Sofía Cándano
Fuelling Data Excellence through the IBM Hyper Protect Accelerator		Global Communications and Branding Lead, Village Capital
Part 2		Ahmed Fadl
Revolutionizing Data Protection: Introducing IBM Hyper Protect Services	10	Program Management Consultant, MENA, Village Capital
Part 3	14	Maddie McElhenny
From Big Data to Big Responsibility: Current Trends in Data Privacy and Technology		Communications Specialist Consultant, Village Capital
Part 4	19	Eva Waweru
Key Sectors: Challenges and Opportunities		Senior Associate, Communications – EMEAA, Village Capital
Part 5	29	Ben Younkman
The Road Ahead		Regional Director, Europe, Village Capital
Reference List	30	
Disclaimer	32	

Cover photo:

Okomera
Friends of Hyper Protect II

Executive Summary

Over the past decade, we've witnessed a transformative shift in how critical services – notably in the financial, educational, and healthcare sectors – are delivered worldwide through new digital platforms. One of the key drivers of this transformation has been the exponential growth of data created, captured, and used worldwide from the now 5 billion internet users. Today, we generate nearly 50 times more data than in 2010, unlocking enormous value and access for stakeholders across the economic spectrum. Unfortunately, the explosion of new data also comes at the cost of reduced privacy. It raises concerns among individuals and business users regarding data protection, security, and regulatory compliance, begging the question: How will companies balance the risks and rewards of mining and protecting these new troves of data?

Building on more than a decade of work with data-driven startups, Village Capital partnered with IBM to leverage IBM's unique and innovative Hyper Protect technology to launch an accelerator program aimed at scaling digital solutions that prioritize data management and protection as core components of their operations. These data-driven startups are pivotal in efficiently addressing global challenges – from driving financial inclusion to underserved and unbanked groups to improving healthcare quality through data insights.

Five years on, the [Hyper Protect Accelerator](#) has supported nearly 200 impact-creating startups, giving us a front-row seat into crucial insights and solutions transforming critical sectors such as healthcare, education, banking, and others. Throughout this report, we share our learnings and discuss how new and emerging trends in data – as well as recent regulations to safeguard it – are shaping relevant industries. We delve into sectors we have seen take off as some of the most promising in this rapidly evolving technology landscape, shed light on the risks and opportunities shaping these sectors, and explore what these changes mean for investors, entrepreneurs, and industry stakeholders in the datatech space.



Ben Younkman
Regional Director Europe,
Village Capital

Part 1

Fuelling Data Excellence Through the IBM Hyper Protect Accelerator



The IBM Hyper Protect Accelerator program was created to identify and support top startups worldwide, leveraging highly sensitive data to build their solutions on the most secure cloud infrastructure in the world.

The investment-readiness and technical mentorship program explicitly helps startups develop and deploy secure cloud-based applications by providing access to IBM's secure cloud infrastructure, tools, and expertise, enabling the companies to accelerate their development process while maintaining high levels of security.

Since its inception in 2019, the program has garnered interest from over 5,000 companies harnessing data to develop innovative solutions. Our team has conducted 800 interviews and supported nearly 200 data-creating companies.





At the IBM Hyper Protect Accelerator, we prioritize and value diversity among the startups we support. We are proud that nearly 40% of our startups have women in leadership roles, and 60% have founders from Black/Brown, LatinX, and Asian communities. Diverse perspectives drive innovation and create a more inclusive entrepreneurial ecosystem.

The IBM Hyper Protect Accelerator program was created to **identify and support** top ventures worldwide, leveraging highly sensitive data to **build their solutions on the most secure cloud infrastructure in the world.**

40%

of our startups have women in leadership roles.



	2019	2020	2021	2022	2023
 Number of Startups	15	30	55	45	45
 Unique Countries	9	13	23	20	23
 Women in Leadership	13%	53%	49%	43%	64%
 Diverse Founders from Black/Brown, LatinX, and Asian communities	33%	53%	62%	76%	60%

As the implementing partner, Village Capital uses its curriculum and network of experts to provide technical, business development, and investor knowledge, preparing startups to scale to the next level.

“

We chose this accelerator because emTRUTH’s vision of data ownership, protection, and privacy is aligned with IBM Hyper Protect. While this is indeed the case, we’ve gotten so much more out of this program. Additionally, interacting with a very diverse and talented cohort of women and persons of color has been insightful and a joy.

”

Irene Woerner, CEO at emTRUTH

The past five years have reinforced and deepened our understanding of how data-creating solutions can revolutionize industries. As entrepreneurs continuously work to develop solutions to local and global challenges, now more than ever, they are creating more inclusive, impact-focused tech products and services – while collecting and sharing private data to do so.



Meet the IBM Hyper Protect Accelerator Startups

<p>FINTECH</p>	<p>HEALTHTECH</p>		
<p>AI</p>	<p>DIGITAL ASSETS</p>		
<p>SECURITY</p>	<p>INSURTECH</p>		
<p>BLOCKCHAIN</p>	<p>BIG DATA</p>	<p>EDTECH</p>	<p>OTHER</p>

Under-Represented Founders

Under-represented founders, particularly Black and female entrepreneurs, face significant obstacles in securing funding. In 2022, Black founders received only about [1% of total venture capital \(VC\) funding in the US](#), while female founders received 1.9%, mix-gender teams 13%, and solely male-founded startups 85%. This stark disparity underscores the urgent need to address these inequities, not only for the sake of fairness but also to democratize the field of innovation and drive economic growth.

Inclusion is crucial in enhancing innovation, as underrepresented founders bring unique perspectives and solutions based on their lived experiences. We're proud to work alongside our partners to bridge this support gap.

As an example of the high-potential innovations we found worldwide, we highlight some remarkable African founders and IBM alumni who collectively raised nearly US \$100 million in startup funding.

Black founders received only

1%

of total venture capital funding in the US in 2022.





Pngme

Operating across Nigeria, Ghana, and Kenya with headquarters in San Francisco, Pngme uses machine learning models trained on billions of data points to optimize lending and reduce risk for financial institutions across sub-Saharan Africa. In 2021, they raised \$15 million in Series A funding for their financial data infrastructure and machine learning-as-a-service platform currently being used by more than 100 institutions, bringing their total investment to \$18.5 million. Pngme's platform caters to fintechs and financial institutions in Sub-Saharan Africa, providing application programming interfaces (APIs), mobile software development kits (SDKs), and a customer management platform to drive personalized user experiences and financial product adoption.



2021 >> **\$15**
million

The company aims to offer data-driven user experiences similar to Alipay and WeChat in China. Pngme allows institutions to collect and aggregate financial data at scale, leveraging machine learning models to analyze and maximize customer lifetime value. Their additional funding allowed them to expand their executive team, enhance their product: Insights Library, and establish more third-party data connections in other markets.



MarketForce

Tesh Mbaabu is the co-founder and CEO of MarketForce, a retail B2B platform based in Kenya, Nigeria, and the US. In 2022, MarketForce raised \$40 million in Series A funding to expand its merchant inventory financing services across Africa. The company planned to introduce buy now, pay later (BNPL) options to help merchants access consumer goods on credit and expand into new markets in East and West Africa. The recent funding round brings MarketForce's total funds to \$42.5 million, including \$2 million raised in a pre-Series A round.

raised
\$40
million
in
2022



Asaak

Ugandan asset financing startup Asaak, founded by Kaivan K. Sattar, raised \$30 million in pre-Series A funding in 2022. The company initially began as an operation to provide loans to farmers and SMEs in 2016 and shifted to motorcycle financing in 2019. Since then, they have acquired over 5,000 motorcycles. Asaak assesses borrowers' creditworthiness using behavioral and financial data, including earnings, trips made, and ratings from highly used platforms like Bolt, Jumia, Safeboda, and Uber. They create a credit score based on this data, allowing borrowers to check their eligibility and apply for financing. As part of its ongoing expansion, the company plans to venture into six additional African markets soon.

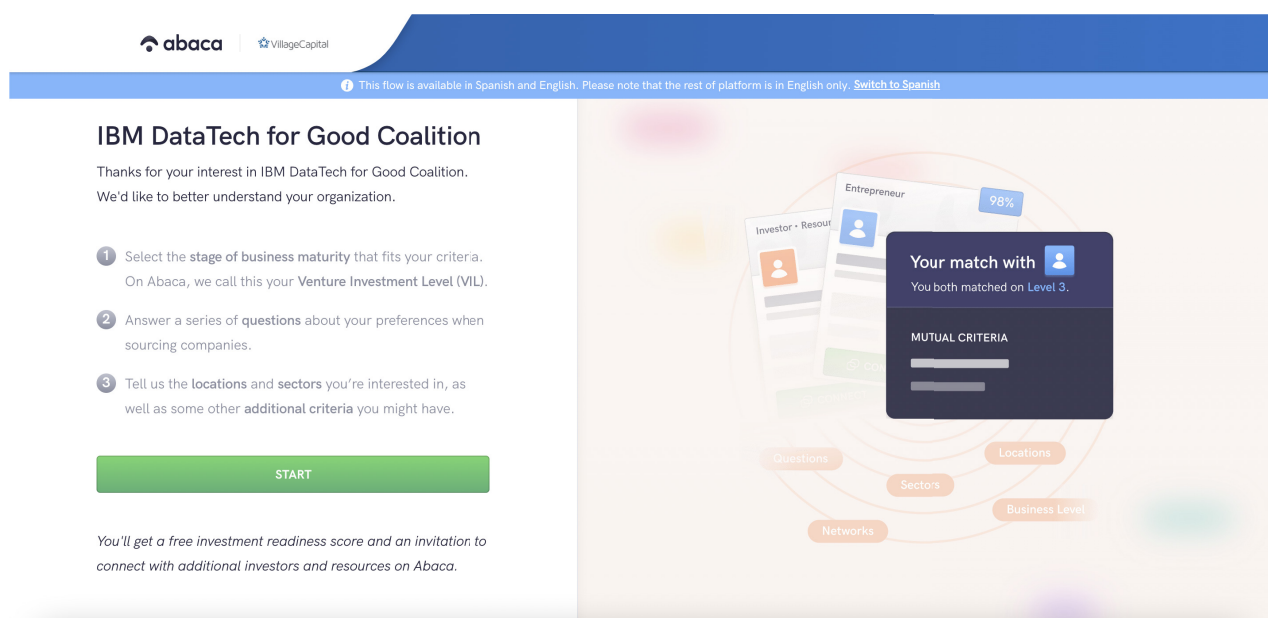
raised
\$30
million
in **pre-Series A**
funding in
2022



Datatech for Good Coalition

To complement the IBM Hyper Protect Accelerator, the [Datatech for Good Coalition](#) was launched in 2020 as an ecosystem of investor support, similarly focusing on startups that utilize highly sensitive customer data for positive societal impact.

The coalition brings together prominent stakeholders and key players involved in developing and supporting impact-creating data solutions. Its primary objective is to establish a platform for valuable discussions and connections, advance the dialogue on data best practices and impact, and highlight innovative ideas across various sectors. To date, the coalition has over 300 members, including 40+ investors active in the verticals the Hyper Protect Accelerator supports.



Join the coalition as an



entrepreneur

or

investor



Part 2

Revolutionizing Data Protection: Introducing IBM Hyper Protect Services

In today's increasingly interconnected and data-driven world, safeguarding sensitive information is critical. [IBM Hyper Protect Services](#) (HPS) represents the culmination of their long-standing expertise in secure computing, ongoing research efforts, and collaborative initiatives. These services provide a groundbreaking solution in cloud computing, providing unparalleled levels of privacy, confidentiality, and regulatory compliance. Launched in 2019, IBM offers its Hyper Protect Services through its cloud infrastructure, designed to operate and function with other cloud service providers.

IBM Hyper Protect Services revolutionizes data protection through advanced security measures, confidential computing techniques, and a trusted infrastructure. These services offer enhanced security, prioritizing data confidentiality and privacy, leveraging IBM's hardware-based security technologies to ensure data remains secure from vulnerabilities and insider threats. They're built on a trusted IBM Z mainframe architecture, providing a resilient foundation, complying with regulatory requirements, facilitating collaboration with academia and industry, and fostering innovation in confidential computing. While IBM Hyper Protect is available on-prem, the program's focus is the offering made available via the IBM Cloud (which is an affordable way to benefit from mainframe architecture without paying to lease a mainframe).

IBM Hyper Protect Services revolutionize data protection through:



advanced security measures



confidential computing techniques



a trusted infrastructure

The two main categories of services available via the public cloud are IBM Hyper Protect Virtual Server ([HPVS](#)) and IBM Hyper Protect Crypto Services ([HPCS](#)).

- **IBM HPVS** provides complete data privacy and protection over your containerized workloads that hold sensitive data or business IP. It is a hyper-secure, flexible server configured for many uses to increase your security and data privacy on the public cloud.
- **IBM HPCS** provides cryptographic services and is ideal for digital assets companies, Quantum-Safe encryption, and multi-cloud key management among other uses. A dedicated cloud hardware security module protects HPCS's cloud data encryption and is compatible with the highest possible security certification: FIPS level 4 (the Federal Information Processing Standard Publication is a US government computer security standard issued by the National Institute of Standards and Technology).



Demystifying Data

Data refers to raw facts, statistics, or information in digital format. It manifests as numbers, text, images, audio, video, or other digital representations. Whether produced by individuals, organizations, or automated systems, data is critical in decision-making and plays a pivotal role in research, innovation, and development across diverse fields and sectors.

There is no question that data has permeated every aspect of our [daily lives](#). From the news we watch, how we navigate our cities, the healthcare we receive, and even our public safety policies, big data analysis shapes the world we live in every day. The volume of data created, captured, and consumed worldwide has significantly grown; we're generating roughly 50 times more data today than we were a little more than a decade ago.

Data exists in various forms, each with its unique characteristics and importance. Here are some of the most commonly used types of data:

PUBLIC DATA
This is non-sensitive and poses no risk when disclosed; hence, it is easily accessible to the general public. It includes information considered public records such as government reports, social media feeds, and publicly accessible web content.
INTERNAL DATA
It is exclusive to an organization, and while not necessarily sensitive, it should be protected. Internal data includes proprietary business information such as financial statements, emails, project documents, and employee records.
CONFIDENTIAL DATA
It is highly sensitive and requires strict access controls and encryption to safeguard its confidentiality. Some examples include customer information, financial data, intellectual property, and trade secrets.
SENSITIVE DATA
This category includes confidential and personal identifiable information (PII) such as credit card information, social security numbers, and medical records. This data requires robust protection to prevent identity theft and privacy harm or violations.

Classifying data helps organizations determine appropriate handling protocols, security measures, and access controls. Organizations can implement effective data protection strategies to mitigate risks and comply with regulations by understanding data sensitivity.

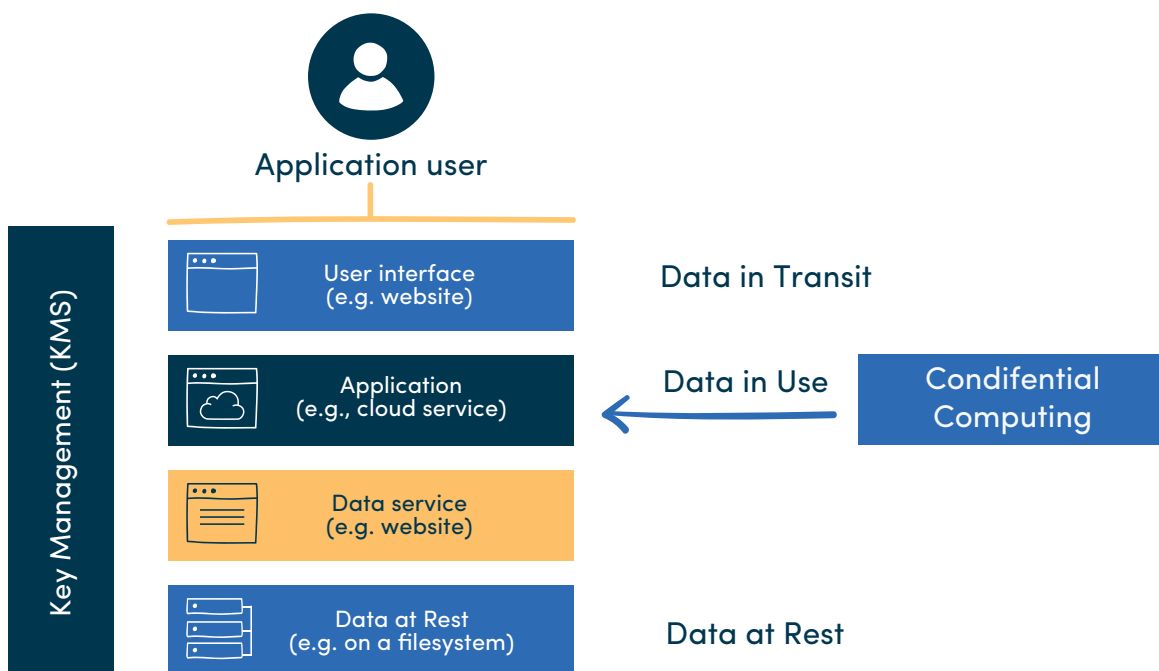


Data Management and Protection Through Confidential Computing

As technology continues to evolve and the volume and complexity of data grow exponentially, the need to secure and protect sensitive data while harnessing its potential as a catalyst for innovation is more significant than ever.

The frequency of cyber attacks is staggering - in 2017, the University of Maryland [conducted a study](#) revealing that a new attack occurs approximately every 39 seconds worldwide, and industry watchdogs have been tracking a dramatic rise in cybercrime during the COVID pandemic ([up 38% in 2022](#)). With the recent surge in ransomware, some experts put the frequency of new cyber attacks occurring every [11](#) to [14](#) seconds in 2023. The financial repercussions are also substantial, as an organization's average cost to recover from a data breach globally is around [US \\$4.35 million](#).

Encryption is pivotal in upholding cloud data security and fostering digital trust. To ensure comprehensive protection, a cutting-edge concept known as confidential computing has emerged. This approach aims to safeguard data at every stage of its lifecycle, including when it is actively processed or utilized by applications.



One of the key technologies enabling confidential computing is secure enclaves. Secure enclaves are isolated and encrypted regions of a processor's memory that allow the execution of sensitive workloads in a trusted environment. They provide strong hardware-based isolation, ensuring that the data and code inside the enclave remain protected and confidential, even from the underlying system and other processes.

By leveraging secure enclaves and other confidential computing technologies, organizations can perform critical operations on sensitive data, such as analytics, machine learning, and artificial intelligence, without compromising privacy or security. It enables scenarios where multiple parties can collaborate on data analysis without exposing the underlying data to each other, enhancing privacy and enabling secure multi-party computation.



Additionally, regulatory compliance, including the General Data Protection Regulation (GDPR) and [PSD2](#) are examples of recent laws in the European Union that either mandate or strongly encourage data encryption at rest and in transit for protection purposes. These laws have also led the EU to emerge as the leader in governance protecting personal information. Similarly, in [Africa and Asia](#), 61% and 57% of the countries have enacted comprehensive data protection legislation, demonstrating a concerted effort to enhance privacy safeguards across the globe.

The Intersection of Data and Impact

The evolving data landscape remains morally neutral. Its influence on society hinges on the ethical and responsible application of information about users' habits, patterns, and behavior, determining whether the transformation is positive or negative. We created the Datatech for Good Coalition to support tech-driven startups using data in ways that benefit society.

Data has numerous opportunities to revolutionize society by creating more inclusive services. Technological solutions that leverage secure data ownership can 1) increase access to essential services, 2) mitigate bias through the equitable use of data, and 3) maintain the protection and privacy of data. We examine each one below.



Increase access to essential services

Data can be a gateway to vital services like healthcare, banking, and transportation. A good example is healthcare, where analyzing health data can pinpoint areas with high disease prevalence, enabling the deployment of medical personnel and aid to regions and communities that would be generally overlooked. Ultimately, this increases access to healthcare and improves the quality of life for people worldwide. Governments should develop fairer and more secure frameworks that lower access barriers for individuals while ensuring their data is protected.



Mitigate bias through equitable use of data

Not all data is created equally – bias can exist in every dataset, and poorly collected data can negatively influence critical decision-making. When the digital world prioritizes the needs of one group, it can further marginalize others. A multifaceted approach involving diverse and representative data sets into algorithms and regular auditing can help identify disparities and enforce fairness within data-driven systems. Data collected equitably can reshape products and services for underserved communities, addressing their challenges and creating new opportunities.



Maintain the protection and privacy of data

Protecting data from hacking or unethical use supports the universal right to privacy and security. Data protection prevents damaging misuse, such as fraud and identity fraud. Upholding data protection and privacy is a fundamental human right.



Part 3

From Big Data to Big Responsibility: Current Trends in Data Privacy and Technology

The growth of meta-data (data that describes other data) across all sectors has led to a spike in hacking and piracy, and heightened the demand for better gatekeepers and systems within the digital ecosystem. Major tech players have assumed this role, ensuring that data is collected and stored securely, with its access heavily regulated.

The surge in meta-data has also catalyzed a boom in the development and application of Artificial Intelligence (AI) and Machine Learning (ML). These technological advancements provide valuable insights and patterns and have revolutionized automation and innovation in various fields. The connection between the growth of meta-data, the emergence of gatekeepers, and the proliferation of AI and ML brings to light the transformative power of today's interconnected world.

Below are other significant trends [industry experts](#) have identified that will shape the data landscape in the coming years.



1. Rise in data privacy legislation and increased need to navigate data management on a global scale.

As of June 2023, “[75% of all countries](#) have implemented some form of data protection rules, and as a result, data sharing and collaboration across borders is becoming increasingly complicated for [global enterprises](#).” While the US does not have a countywide federal regulation on privacy, there is a wave of privacy regulations set to go into effect in key states across the US throughout 2023, indicating the increasing importance of data management and oversight across all industries. Mo Plassing, Chief Product Officer at [Immuta](#), predicts that “data localization challenges will continue to



**of all countries
have implemented
some form of data
protection rules.**



evolve as requirements and the geopolitical climate change, and the space will only become more complicated as data volumes and sources continue to grow, and regulations become increasingly stringent.”

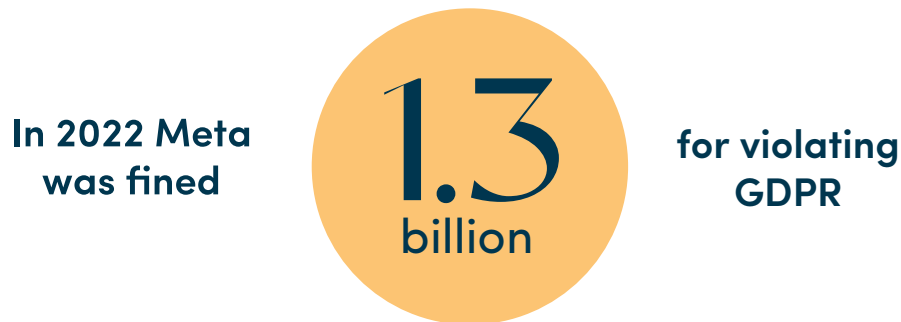
It’s controversial that although the US and Europe have stricter privacy and data protection laws than in Africa and Latin America, most data breaches still happen in these regions. This discrepancy highlights possible weaknesses in implementing or enforcing these regulations and casts doubt on their efficacy. It also emphasizes the need to continuously evaluate and improve data protection measures worldwide to guarantee the security and privacy of people’s information.

2. The cost of compliance is rising, accompanied by more severe financial consequences for businesses.

The record-setting \$1.3 billion fine that the EU issued to Meta in 2023 for violating the GDPR indicates the growing scrutiny tech firms face around their data compliance. There’s hardly a month that goes by without a significant report on a massive data breach or weighty fine leveled against a tech firm and organizations for violating a bundle of data privacy laws.

In the US, California’s Attorney General issued a \$1.2 million fine [against Sephora](#) for violating the California Consumer Protection Act (CCPA). Sephora had failed to a) treat its transfer of consumer data as a “sale”, b) process consumers’ opt-outs of that sale as indicated by a universal opt-out signal, and c). address these violations within a 30-day period.

The state has also rolled out its enforcement agency, [the California Privacy Protection Agency \(CPPA\)](#), with states like Virginia, Colorado, and Utah enacting new data privacy laws. The price tag for companies mismanaging user data will only go up in the future.



However, according to [privacy advocates](#) and [data protection authorities](#), many believe that GDPR’s enforcement does not go far enough, and the regulatory gaps have prompted the EU to draft and launch more comprehensive policies like the newly passed [Data Act](#), which will lead to more vigorous enforcement and higher penalties in the years to come.

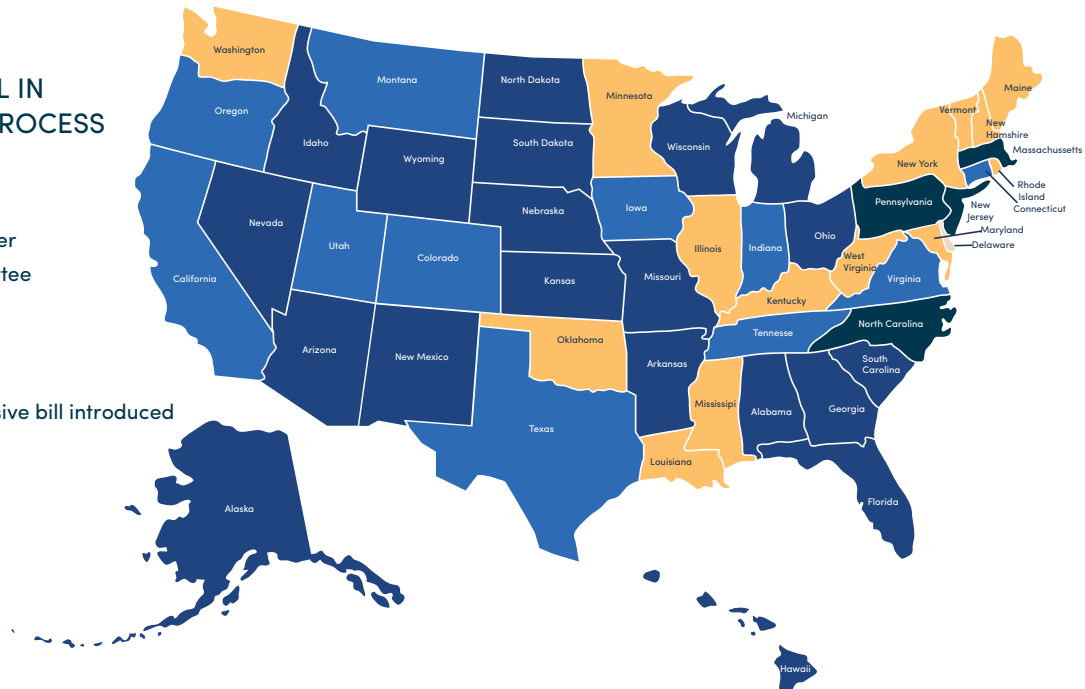
As of January 2023, European data regulators issued [€1.64 billion in fines](#) for GDPR violations, a 50% increase from 2021. They are on track to give a record amount of financial penalties as they tighten enforcement and oversight. US data privacy regulations are behind Europe’s more sweeping GDPR framework. A host of new state laws will go into effect in 2023; early signs indicate that these new laws can have profound financial implications for non-compliant companies.



US State Privacy Legislation Tracker 2023

STATUTE / BILL IN LEGISLATIVE PROCESS

- Introduced
- In committee
- In cross chamber
- In cross committee
- Passed
- Signed
- Inactive bills
- No comprehensive bill introduced



Source: International Association of Privacy Professionals

🕒 Last update: 8/46/2023

3. SGBs will also need internal data privacy compliance measures.

While large companies pose the greatest risk of data privacy violations, the regulatory landscape is changing, and we're seeing Small and Growing Businesses (SGBs) face increased scrutiny from privacy regulators. GDPR regulators have seen fit to issue fines [as small as €28](#). As components of the Data Act roll out across the EU and the US, state legislation like the California Consumer Privacy Act (CCPA) will also expose regulatory compliance risk among smaller players. Under the newly rolled out CCPA, businesses processing the personal information of more than 100,000 California residents or households will be subject to the law (among other requirements). This means that even SGBs with a modest digital presence will need to comply as soon as possible and develop internal privacy programs to avoid fines with the potential to strangle their growth at an early stage.

4. Companies will need to balance data protection and portability.

Data portability, which refers to the ability to move data sets between platforms or service providers without altering their content, is poised to become a big concern for businesses that are increasingly transitioning to cloud-based services and migrating between different or multiple cloud-service providers based on the location, sensitivity and regulation of the data. As companies have an increasing suite of incentives from various cloud-service providers while facing increasing regulatory scrutiny, many global enterprises are trying to understand if migrating some or all of their data to a new cloud-hosted provider will mean they retain all of their data and the same level of privacy and protection after the transition.

These concerns highlight the need for gatekeepers to delicately balance privacy and portability, enabling organizations to remain compliant as they navigate the evolving landscape of cloud-based data management.



“

Over the past five years, we noticed that revamping internal systems was challenging and costly, especially for SGBs looking to transition between providers and cloud-based services. They wanted the ability to seamlessly move data without altering its content. We've made significant progress lowering those technical barriers through our cloud services, reaching a point where accessibility and security are now a key component with data portability.

”

Adam LG Ring, Global Head IBM Hyper Protect Accelerator

5. AI and ML will increasingly impact data privacy legislation.

AI and ML can have both positive and negative impacts on data privacy. On the one hand, they enhance data protection by identifying patterns of suspicious behavior in real time, aiding the early detection of potential data breaches. On the other hand, hackers can use them to analyze large data sets and build very detailed profiles, which could lead to unauthorized access, identity theft, and other privacy violations.

A good example is the rapid advancements in AI's ability to replicate reality, which have ignited significant concerns about the need for effective regulation. With technology companies [granting individuals](#) the power to generate convincingly realistic fake images, synthetic audio, video, and human-like text, the potential for misinformation and deception has reached unprecedented levels.

Striking a balance between innovation and safeguarding personal information is a critical task that will require innovative solutions and robust regulatory frameworks to ensure that privacy remains intact in an era of increasingly sophisticated AI and ML-generated content. In the US, at least [17 states](#) have already introduced AI-related legislation.



6. The notion that data is the new oil has lost its relevance.

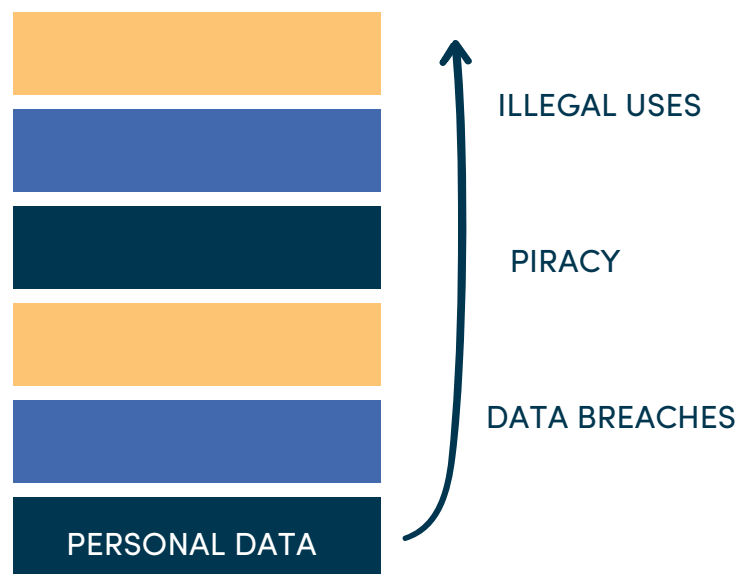
In May of 2017, [The Economist](#) released an article that famously popularized the idea that “the world’s most valuable resource was no longer oil, but data” – a phrasing that has become almost cliché in speculations on the growth of the digital economy. However, when British mathematician Clive Hummerly first coined the concept of “data as the new oil” in 2006, he was arguing that data, [like oil, data isn’t helpful in its raw state](#) – it has to be processed and refined before it can be useful.

While companies like Facebook (now Meta), Amazon, Apple, Netflix, and Google (FAANG companies) have grown empires built on mining and refining user data for the past three decades and are now the biggest targets of data privacy regulators, they are also facing growing resistance from users to turn over their data for free and increasing skepticism from users and legislatures alike on how personal information is being used and shared by tech, financial, and health companies. Data privacy advocates at [Osano](#) argue that “Data is valuable, but the comparison to oil does away with any nuance and ignores the reality of modern digital businesses. While personal data collection has fueled [FAANG companies] growth, it hasn’t come without additional risk and management requirements.”

As the collection of personal data piles up, so do data breaches, piracy, and the multiple examples of illegal use we have highlighted throughout this report. Regulators see this growing tide of data as a potential disaster and are trying to increase the cost to companies for poor data infrastructure, lax compliance, and outright regulatory violations. In the past, companies collected data at all costs. Now, the increasing cost of breaches and regulatory oversight pushes these same companies to become selective about the data they collect and how they store it.



Regulators see this a potential disaster waiting to happen.



Part 4

Key Sectors: Challenges and Opportunities

Startups are uniquely positioned to rebuild consumer trust through privacy-focused, intentionally secure alternatives and leverage sensitive data to improve the quality of and access to digital, financial, and healthcare services. Over the past five years, IBM Hyper Protect Accelerator has supported over 200 startups, creating equitable opportunities and solutions for the underrepresented. The goal is to help those at the forefront of technology venture into uncharted territories. Their impact is profound. And this is just the beginning.

Below, we dive into the key sectors and highlight the groundbreaking startups advancing this space.



Sector 1: Healthtech

The Challenge

Systemic flaws are plaguing the global healthcare industry. Rising costs burden individuals, families, and governments. Unequal access causes disparities in health outcomes based on socioeconomic status, geographic location, and demographic factors. Fragmented systems between providers, institutions, and sectors need more coordination and integration of communications, data, and interoperability. Complex regulatory and bureaucratic frameworks slow innovation and the approval of new treatments or technologies. All of this amounts to subpar quality of healthcare services to humans.

Healthtech – or the development and application of technologies and digital innovation in the health industry – has emerged to find solutions to improve the quality of healthcare processes, delivery, and patient outcomes. Due to the digitization of the healthcare system from the pandemic, more



medical data is stored and shared virtually through electronic health records (EHRs), medical devices, wearables, and research studies than ever before.

When we turn large volumes of data into actionable insights, we can streamline processes, reduce barriers to information sharing, and expand the reach of healthcare services, ultimately improving access to timely and quality care for underserved individuals and communities.

However, the data collection and sharing practices come with risks, including inconsistencies and limited communication means between systems, such as electronic medical records, medications, labs, and others, exacerbating data silos and biases. Additionally, health records contain sensitive personal information, making them an attractive target for hackers. Each data exchange and transfer point becomes a potential vulnerability, especially as virtual sharing of medical data continues to grow.

The Opportunity

Healthcare data can be more integrated and interoperable when leveraged safely and securely to improve access, lower costs, and boost outcomes. New technologies like AI and ML equitably advance early detection and personalized treatments.

Industry transformation requires a balance between the benefits of data sharing and interoperability and the need for stringent security measures to protect it. It also requires disruptive technologies and solutions addressing inequities, collaboration between healthcare organizations, technology providers, policymakers, and cybersecurity experts, comprehensive strategies, and frameworks. A vibrant ecosystem of startups and entrepreneurs is at the forefront of these solutions. Supporting and investing in them will empower stakeholders to embrace practices and behaviors that enhance inclusivity and affordability in quality healthcare.



Case Study



Telebionix, a US-based company, is revolutionizing the healthcare industry through monitoring daily health, utilizing AI-driven insights, and facilitating seamless communication with caregivers – all from the comfort of home. Their mission is simple: improve access to healthcare and, in turn, save lives.



Telebionix's product is Remosense, a clinical-grade, smart, handheld device whereby patients accurately measure seven vital signs, such as heart rate, blood pressure, and body temperature, and instantly relay them to their physician. The app transmits data securely and stores it in their HIPAA, GDPR, ISO, and ISO-compliant cloud. Physicians translate that patient data into actionable to provide direct care. Telebionix improves the quality of diagnoses and care by improving the quality of data.

In addition to improved patient care, Remosense prioritizes equitable access to healthcare, particularly in underserved communities and remote areas. Furthermore, it offers physicians new revenue streams and extends patient care beyond their practice. Lastly, it improves the overall experience for both patients and healthcare providers, providing a foundation for a strong and healthy relationship.

Widy Medina founded Telebionix in 2020, combining his background in healthcare (medical devices and pharmaceuticals) with tech such as robotics, product design, fabrication, automation, electronic assembly of consumer products, and biotech. Similarly to the other founding members, he understood the challenges and impact of lacking access to healthcare and technology's power to save lives.

Telebionix has raised \$600,000 in capital to date and has been recognized as a leader in MedTech through "IFAH," "Most Fundable Companies," "Open Business Council Awards," and "Open AI." They were also ranked "Most Fundable Company" by Pepperdine Graziadio Business School.





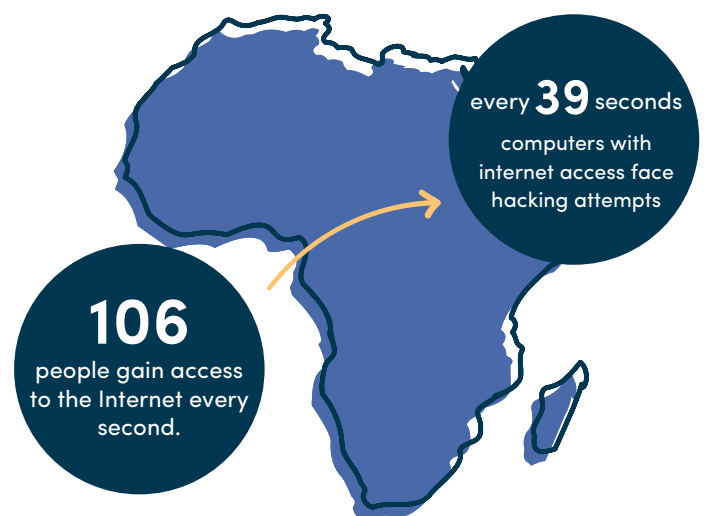
Sector 2: Fintech

The Challenge

Like healthcare, the global financial system faces several key challenges that impact its stability, efficiency, and inclusiveness. Between economic volatility, systemic risk, regulatory compliance, and unethical practices, underserved populations face inequitable access to finance. While we saw significant progress in financial inclusion between 2011 and 2017, when [1.2 billion people](#) worldwide gained access to financial accounts, over 1.7 billion unbanked people still lack access to wealth-building opportunities. Roughly 50% of the unbanked are women from impoverished households in rural areas or out of the workforce. Financial inclusion is critical not only for individuals, families, and businesses to store money, manage payments and cash flows, generate savings, access credit, and make investments but also for communities, nations, and the entire global system to improve economic opportunities and outcomes.

Data has enormous potential to drive equitable access to finance. However, even when people have access to financial products and services, their data carries the risk of exploitation that can lead to further exclusion. Cyber attacks have [tripled](#) over the last decade, and financial services remain the most targeted industry.

Let's look at Africa, where fewer than half of the African countries have laws to protect personal data. In Sub-Saharan Africa, in particular, 106 people gain access to the Internet every second, while computers with internet access face hacking attempts [every 39 seconds](#). Efforts to promote financial inclusion must go hand in hand with protecting data integrity and reinforcing cybersecurity measures.



The Opportunity

The rise of fintech – integrating digital technology and finance to enhance financial services, including banking, payments, insurance, investment, and more – is revolutionizing sector operations. Specifically, the [advancement of digital technologies](#), from 5G, the [Internet of Things](#), [blockchain](#), AI, big data, and substantial developments in data storage and management, has significantly increased efficiency, security, and accessibility. Through privacy protection, regulatory compliance, inclusive access to data-driven services, among others, digital financial breakthroughs can open up new possibilities for people worldwide.

Still, there is a long way to go. Once again, startups and entrepreneurs are filling critical inequity gaps. Startups in this sector have grown exponentially, providing financial services to customers in [innovative yet secure](#) ways. With the emergence of cryptocurrencies, digital wallets, crowdfunding, peer-to-peer lending, and more, these companies are leveraging machine learning technology, big data, cloud computing, and cryptographic methods to lower barriers to access by reducing costs and extending services to the most vulnerable and underserved, while enhancing the physical, data and financial infrastructure.

Case Study



[Asaak](#) is a global fintech company based in Uganda and Mexico, offering asset financing to marginalized small and medium business owners. Initially founded in 2016 to lend to farmers, they have focused on helping small-to-medium-sized enterprises gain access to finance since 2019 through safely and securely leveraging data.



“Bodas,” or motorbike taxis, are a popular transport mode across Africa, especially in major cities like Kampala. Asaak primarily works with its drivers, or “bodaboda operators,” who traditionally lack access to traditional banking services due to strict income history and account activity requirements. In particular, because they don’t have government-issued identification and are not literate, they are either employed by bike owners or rent or lease their bodas, both of which can be predatory business models.



“

A typical East African boda driver grew up in a village doing agriculture and dropped out of school early to support his family. They are usually not literate, do not have internet access, and often do not even have government-issued ID. Asaak takes up the considerable task of making the unbankable creditworthy, which we do by giving financial literacy and defensive driving training to our clients before they can receive a motorcycle from us. As a direct result of our product, we double the income of every driver we work with. Before the driver came to us, he was paying 50% of his income for rent on a bike that he would never have owned.

”

Kaivan Sattar, CEO and Founder at Asaak

Asaak enhances motorcycle ownership through alternative data. They partner with various mobility and e-commerce platforms – like Bolt, Jumia, Safeboda, and Uber – to leverage behavioral and financial information, including their earnings, trip history, and ratings. Asaak then turns this data into a credit score for their borrowers, giving them full transparency into qualifying for finance. Kaivan shares that “Drivers usually receive motorcycle financing (about \$1,500 worth of credit) within three days of signing up and pay an interest of 1 to 4% depending on their credit score.” Asaak also provides financial literacy and defensive driving training to ensure the bodaboda operators responsibly care for their motorbikes.

Asaak has expanded its product offerings to fuel and smartphone loans, empowering business owners on upward mobility to improve their income opportunities and better provide for their families.

Kaivan Sattar, CEO and founder, shares that Asaak benefited tremendously from the IBM Hyper Protect program.

“

We received a thought partnership to build our Luganda language chatbot to better engage with our customers who are not smartphone users and are not literate yet pay their loans on time. We are developing a system to input and output spoken Luganda to serve our customers faster.

”

Kaivan Sattar, CEO and Founder at Asaak

To date, Asaak has secured \$30 million in pre-Series A equity and debt funding. In 2022, they had disbursed over 11,000 motorbikes. They plan to enter several new emerging markets to expand operations and impact.

With Asaak

drivers have
double
their income.

Before, they use 50% of their income for rent on a bike they would never have owned.





Sector 3: Datatech

The Challenge

Recent technological advancements, increased internet usage, and the digitalization of various industries have led to an exponential surge in digital data collected, processed, stored, and consumed today. The global volume of data grew from 2 ZetaBytes in 2010 to 79 ZetaBytes in 2021. Experts predict it will reach 163 ZetaBytes in 2025 and [\\$156.72 billion](#) in 2026. Every human action – including non-digital – gets aggregated as a data point by various organizations (corporations, government, social media platforms, etc.) as part of their operations.

Digital and traditional industries, including healthcare, transportation, energy, media, retail, manufacturing, and more, increasingly rely on access to data to provide valuable insights to influence their strategies and growth models. Furthermore, individual users have ongoing questions and concerns regarding their personal data protection, security, and ownership. Specifically, data ownership is the right and ability to access, modify, use, monetize, and delete a piece of data, which plays a central role in maintaining data privacy and security.

While the digitalization of data can be incredibly useful in helping various stakeholders make decisions, it can also exacerbate global inequities in the following ways:

- The data is often disconnected across systems and platforms between organizations, hindering interoperability and integration and risking data quality and accuracy issues.
- It can create a digital divide between those with access to it and those without, exacerbating disparities in accessing information and opportunities.
- Bias and discrimination exist in all data, which can be reflected in algorithms and AI systems, leading to one-sided outcomes for underrepresented communities.
- The data is owned and controlled by a few powerful entities, all of whom can limit access, control, and benefits.

The need for solutions to promote digital inclusion, address biases in data and algorithms, and ensure equitable access to and control over data are critical.



The Opportunity

[Datatech](#) is the development of technological products and services that harness the power of big data analysis, AI, and machine learning algorithms to enhance and optimize various market sectors. These developments help to manage large amounts of data by building solutions for data management through collection, storage, analysis, interpretation, and utilization.

Secure data ownership opens the door for cross-collaboration between different organizations (delegated data owners), allowing individual users to access essential services such as healthcare, financial services, among others. Startups and entrepreneurs are developing new data technologies to build better, more inclusive, impact-focused tech products and services to leverage secure data ownership to enhance access to vital services while ensuring equitable data usage to mitigate bias and safeguard data privacy.

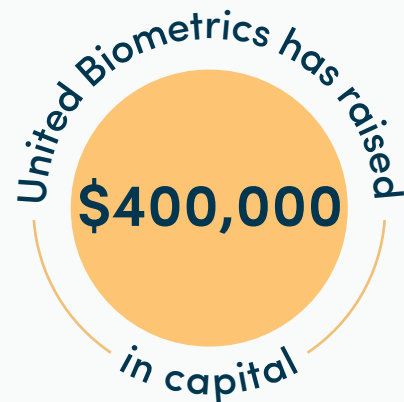
Case Study



[United Biometrics](#), based in France, is a leader in the cybersecurity vertical of the data sector, creating digital authentication solutions across all industries, enabling banks, corporations, and governments to protect their applications, data, and network access.

They specialize in creating authentication and access management software products for mobile and fixed devices to prevent security concerns like fraud, cyber-attacks, and terrorism. In doing so, their solutions require a robust authentication platform based on multiple biometric factors like fingerprint, voice, and face, which helps organizations safeguard their critical applications, from payment platforms to mobile payments, online banking portals, financial IT assets, data centers, IoT, Factory 4.0 and the blockchain.

Co-founders Christopher Richard and Yves Chemla launched the company in 2014.





Sector 4: Digital Assets

The Challenge

Digital assets refer to any content or value in a digital format containing inherent ownership rights or economic value. For example, think of digital currencies, cryptocurrencies, digital tokens, digital art, music files, e-books, software, domain names, digital contracts, and other digital files or records. These assets are typically stored and managed using digital technology, such as blockchain, distributed ledger technology, or centralized digital platforms. They are sold, exchanged, or used as a medium of value transfer through digital platforms or marketplaces.

Data security and privacy are vital in digital assets to protect sensitive and valuable data from unauthorized access, breaches, and malicious activities. As a result, many jurisdictions have enacted data protection laws and regulations to safeguard individuals' privacy rights and promote responsible data handling. Adhering to these practices is not only an ethical obligation but a legal one.

The Opportunity

Startups and entrepreneurs across different sectors are developing innovative solutions that bolster security, manage risks, and ensure compliance with data protection regulations. Their focus spans cybersecurity, encryption, blockchain, data privacy, and beyond. Their end goal? Foster a more inclusive and secure digital environment globally.

In 2022, the IBM Hyper Protect program partnered with the Newmoon Accelerator, which aims to support those working with [blockchain technology](#) to bring about positive change worldwide. Specifically, Newmoon addresses real-world issues such as environmental degradation, creator ownership rights, transparent governance models, and educational and commerce inequality. In areas such as fashion, art, music, gaming, metaverses, e-commerce, and decentralized autonomous organizations (DAOs). Newmoon leverages its unique ability to introduce positive technological ideologies, initiatives, and products into industries that have traditionally been resistant to change.



The ability to connect with and utilize the existing real-world infrastructure and tap into global resources and talent like IBM has played a transformative role in maximizing the impact of these projects at every stage, from ideation and development to implementation. The knowledge and expertise in decentralized aspects of blockchain and technology provide new opportunities to attract talented and dedicated developers working tirelessly to address critical global challenges.

Through the collaboration with Newmoon, we identified eight digital assets companies to support their growth and impact. NeftyBlocks is one of those companies leveraging blockchain technology to ensure digital assets' authenticity, ownership, and provenance.

Case Study



NeftyBlocks, based in Guatemala, is a platform that allows users to create, buy, and sell Non-Fungible Tokens (NFTs). NFTs are unique digital assets – each with authenticity, transparency, and immutability – representing various forms of digital content, such as artwork, music, videos, virtual real estate, and more. Their user-friendly interface enables artists, creators, and collectors to mint their NFTs, showcase their collections, and participate in the marketplace through trading and sales.

Many of these artists historically lacked access to the marketplace. However, NeftyBlocks is lowering the entry barrier by no longer requiring technical partners to participate in the digital economy through revenue-generating possibilities. Artists can earn royalties on secondary sales, generating ongoing income as the value of their creations appreciates. This model is especially beneficial for underrepresented artists who have historically faced challenges monetizing their work or receiving fair compensation. Many creators have approached them, claiming that because of what NeftyBlocks is doing, they are able to make a living from their art.

While doing so, blockchain technology ensures digital assets' authenticity, ownership, and provenance, resulting in a decentralized, transparent, and inclusive ecosystem. They're driving innovation in the digital art and content industries, fueling the growth and evolution of the NFT market.

NeftyBlocks has raised \$970,000 in capital and generated \$500,000 in revenue.



The Road Ahead

Our vision is for datatech solutions to close the massive equity gap worldwide, enabling all access to critical products and services. Specifically for the digital, financial, and healthcare sectors, investing in and supporting the companies at the forefront of these solutions will revolutionize the industries in ways we've never seen before.



The impact is real.

Together, we can pave the way for a truly equitable and inclusive future through continued support.

Join us!

Join the coalition

Become a mentor

Fund a partnership



Reference List

1. Davis, D.-M. (2023b) Women-founded startups raised 1.9% of all VC funds in 2022, a drop from 2021, TechCrunch. Available at: <https://techcrunch.com/2023/01/18/women-founded-startups-raised-1-9-of-all-vc-funds-in-2022-a-drop-from-2021/>
2. Davis, D.-M. (2023a) Women-founded startups raised 1.9% of all VC funds in 2022, a drop from 2021, TechCrunch. Available at: <https://techcrunch.com/2023/01/18/women-founded-startups-raised-1-9-of-all-vc-funds-in-2022-a-drop-from-2021/>
3. April 30, 2020 (2021) Eight Ways Big Data Affects Your Personal Life, Michigan Technological University. Available at: <https://onlinedegrees.mtu.edu/news/ways-big-data-affects-your-personal-life>
4. Hackers attack every 39 seconds (2020) Security Magazine RSS. Available at: <https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds>
5. Anderson, J.L. (2023) Global cyberattacks increased 38% in 2022, Security Magazine RSS. Available at: <https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022>
6. Ransomware attacks, a growing threat that needs to be countered (no date) United Nations : UNODC Regional Office for Southeast Asia and the Pacific. Available at: <https://www.unodc.org/roseap/en/2021/10/cybercrime-ransomware-attacks/story.html>
7. The latest Cyber Crime Statistics (updated October 2023): Aag it support (2023) AAG IT Services. Available at: <https://aag-it.com/the-latest-cyber-crime-statistics/>
8. Cost of a data breach 2023 (no date) IBM. Available at: <https://www.ibm.com/reports/data-breach>
9. Communications (2023) Everything you need to know about PSD2: BBVA, NEWS BBVA. Available at: <https://www.bbva.com/en/everything-need-know-psd2/>
10. Data Protection and Privacy Legislation Worldwide (no date) UNCTAD. Available at: <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>
11. Fadl, B.Y. and A. (no date) Exploring the intersection of impact and data privacy: Conversations with Fintech, Healthtech, and ethical AI startups at IBM ZDAY, News & Views • Village Capital. Available at: <https://newsandviews.vilcap.com/posts/the-intersection-of-impact-innovation-and-data-privacy-conversations-with-fintech-healthtech-and-ethical-ai-startups-at-ibm-zday>
12. Matt Davis, C. (IAPP) (2023) 5 emerging data privacy trends in 2023, The Intuitive Data Privacy Platform for Simplifying Compliance. Available at: <https://www.osano.com/articles/data-privacy-trends>
13. Localization of data privacy regulations creates competitive opportunities (2022) McKinsey & Company. Available at: <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities>
14. Drenik, G. (2023) Data Security & Privacy Trends for 2023, Forbes. Available at: <https://www.forbes.com/sites/garydrenik/2023/02/02/data-security--privacy-trends-for-2023/?sh=c72fd9b64626>
15. Homepage (2023) Immuta. Available at: <https://www.immuta.com/>
16. Matt Davis, C. (IAPP) (2023) An analysis of the Sephora Enforcement Action, The Intuitive Data Privacy Platform for Simplifying Compliance. Available at: <https://www.osano.com/articles/sephora-enforcement-ccpa-analysis>
17. Staff, O. (2023) Meet the california privacy protection agency (CPPA), The Intuitive Data Privacy Platform for Simplifying Compliance. Available at: <https://www.osano.com/articles/california-privacy-protection-agency>
18. Burgess, M. (2022) How GDPR is failing, Wired. Available at: <https://www.wired.com/story/gdpr-2022/>
19. Lomas, N. (2023) Big changes coming for GDPR enforcement on Big Tech in Europe?, TechCrunch. Available at: <https://techcrunch.com/2023/01/31/gdpr-enforcement-reform-dpa-oversight/>
20. The european data act (no date) The European Data Act. Available at: <https://www.eu-data-act.com/>
21. Woollacott, E. (2023) GDPR fines reach record level, Forbes. Available at: <https://www.forbes.com/sites/emmawoollacott/2023/01/18/gdpr-fines-reach-record-level/?sh=6a22f790652d>
22. (No date) Global Comprehensive Privacy Law Mapping Chart. Available at: <https://iapp.org/resources/article/global-comprehensive-privacy-law-mapping-chart/>



23. GDPR fines list: Find all GDPR fines & detailed statistics (2022) Privacy Affairs. Available at: <https://www.privacyaffairs.com/gdpr-fines/>
24. Bond, S. (2023) It takes a few dollars and 8 minutes to create a deepfake. and that's only the start, NPR. Available at: <https://www.npr.org/2023/03/23/1165146797/it-takes-a-few-dollars-and-8-minutes-to-create-a-deepfake-and-thats-only-the-sta>
25. Report legislation related to Artificial Intelligence (no date) National Conference of State Legislatures. Available at: <https://www.ncsl.org/technology-and-communication/legislation-related-to-artificial-intelligence>
26. The world's most valuable resource is no longer oil, but Data (no date) The Economist. Available at: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>
27. Suarez-Davis, J. (2022) Data isn't 'the new oil' - it's way more valuable than that, The Drum. Available at: <https://www.thedrum.com/opinion/2022/12/12/data-isn-t-the-new-oil-it-s-way-more-valuable>
28. Argyres, D. et al. (2022) Digital Health: An opportunity to advance health equity, McKinsey & Company. Available at: <https://www.mckinsey.com/industries/life-sciences/our-insights/digital-health-an-opportunity-to-advance-health-equity>
29. Telebionix ranked most fundable company by Pepperdine Graziadio Business School (no date) Landkit. Available at: <https://telebionix.com/blog-post-1.html>
30. Overview (no date) World Bank. Available at: <https://www.worldbank.org/en/topic/financialinclusion/overview>
31. Kristalina Georgieva, I.M.D.C. on F.I. and C. by I.M.F. (2020b) Financial Inclusion and cybersecurity in the Digital age, IMF. Available at: <https://www.imf.org/en/News/Articles/2020/12/10/sp121020-financial-inclusion-and-cybersecurity-in-the-digital-age>
32. Kristalina Georgieva, I.M.D.C. on F.I. and C. by I.M.F. (2020a) Financial Inclusion and cybersecurity in the Digital age, IMF. Available at: <https://www.imf.org/en/News/Articles/2020/12/10/sp121020-financial-inclusion-and-cybersecurity-in-the-digital-age>
33. Elsaid, H. (2023) 5 factors driving the rise of fintech in the financial services industry , Trade Finance Global. Available at: <https://www.tradefinanceglobal.com/posts/5-factors-driving-rise-fintech-financial-services-industry/>
34. Internet of things (2023) Trade Finance Global. Available at: <https://www.tradefinanceglobal.com/tradetech/internet-of-things-iot/>
35. Remarks by Deputy Managing Director Mitsuhiro Furusawa for the Conference on Financial Inclusion in West Africa (2016) Financial inclusion: Bridging economic opportunities and outcomes, IMF. Available at: <https://www.imf.org/en/News/Articles/2016/09/20/sp092016-Financial-Inclusion-Bridging-Economic-Opportunities-and-Outcomes>
36. Njanja, A. (2022) Ugandan Fintech Asaak raises \$30million to support acquisition of motorbikes, smartphones by taxi operators, TechCrunch. Available at: <https://techcrunch.com/2022/01/17/ugandan-fintech-asaak-raises-30million-to-support-acquisition-of-motorbikes-smartphones-by-taxi-operators/>
37. Research and Markets (2018) Global Big Data Market Forecast to 2026: An \$156.72 billion opportunity, GlobeNewswire News Room. Available at: <https://www.globenewswire.com/news-release/2018/11/15/1652475/0/en/Global-Big-Data-Market-Forecast-to-2026-An-156-72-Billion-Opportunity.html>
38. Datatech: What is it - definition: Blog Onaudience.com (2022) On Audience. Available at: <https://www.onaudience.com/resources/what-is-datatech/>
39. IBM Hyper Protect Accelerator Hub - group home (2022) IBM Hyper Protect Accelerator Collaboration with the Newmoon Accelerator. Available at: <https://community.ibm.com/community/user/ibmz-and-linuxone/blogs/ahmed-fadl2/2022/06/22/ibm-hpa-collaboration-with-newmoon-accelerator>



Disclaimer

This document was prepared by analysts at Village Capital for general information purposes only and is not necessarily definitive, current, or authoritative, and is not intended to be used, read or consumed as investment advice. Data used in this document was gathered from reliable sources, but the analyst(s) and the publishers of this document do not hold themselves responsible for the accuracy or completeness of the data used. The document provides the opinions, analyses, and conclusions of Village Capital analysts only and is provided without any warranties of any kind. Village Capital and its partners do not in any way endorse the findings, views and conclusions in this document. We do not accept any liability for any direct or remote loss or damage arising out of the use of all or any part of the information contained in this document.

USE OF THIS PUBLICATION FOR THE PURPOSE OF MAKING INVESTMENT DECISIONS EXPOSES YOU TO SIGNIFICANT RISK OF LOSS.

Reception of this publication does not make you a client or provide you with the protections afforded to clients of Village Capital. When distributing this document, Village Capital is not acting on behalf of the recipient of this document and will not be liable for providing investment advice to any recipient in relation to this document. Accordingly, Village Capital will not be held accountable to any recipient for providing the protections afforded to its clients.

This document is published for information purposes only and is not an offer to solicit, buy, or sell any security or other similar instruments or investments of any kind. This document does not provide investment advice and should not be used as such under any circumstances. It has been prepared without regard to the individual financial circumstances and risk and return objectives of individuals who receive it.

© Village Capital 2021. All Rights Reserved. This note has been prepared by Apoorv Karmakar and the Village Capital Communications Department. For questions, please contact: info@vilcap.com, Village Capital, 740 15th St. NW, Suite 301, Washington, DC 20005.

