Digital Distrust

A fundamental flaw in the Information Technology Frame-work

A PUBLICATION OF Hiving Technology

Author: Gert Botha

Date: July 2018

Hiving

Enabling my World

Introduction

Trapped in a framework that promotes distrust

The world is becoming increasingly digital and we're powerless to stop it. We shop online, we pay our bills on our smartphone or computer, and our medical records and personal data is stored digitally. But do we really trust that the information stored is accurate? Can we be sure our digital transactions won't be compromised? Do we trust that our personal information is safe and secure? Are the things we see and read even real? How do we know? These questions and concerns have given rise to a concept known as Digital Trust. But what does it really mean?

Digital Trust can be defined as the process to establish and manage the myriad of digital interactions and relationships between governments, businesses, individuals and things. Digital Trust is not only about trusting the digital transactions themselves, but also trusting the digital landscape in which they function and operate. Trusting digital content used to make decisions, as well as trusting that technology interactions will have a safe, predictable outcome irrespective of the application or purpose, is all part of Digital Trust.

After decades of using information technology, we have never stopped to question the fundamental principles the IT framework was built on. Challenges such as security, privacy, poor data quality and integrity, multiple unauthenticated identities and others have been addressed by building tools, workarounds and fixes -- rather than questioning the core principals and repairing the foundation. After decades of rapid technology development and evolution, **we are trapped in a framework that promotes Digital *Distrust***.

TABLE OF CONTENTS

1 Current Reality

"Privacy, Security, and Trust"

Current Reality

The public's unbridled enthusiasm for all things digital has been tempered by concerns about privacy, security, and trust. People are becoming increasingly aware that online information is not necessarily true, whether it appears as user reviews, advertisements, news or search results. Social media too, is vulnerable to manipulation by hackers or foreign powers who influence perceptions, as was recently illustrated by the case with Facebook & Cambridge Analytics. There are plenty of examples of data breaches too, including: (1) 92 million people's data with My Heritage- the ancestry site that match peoples DNA (2) 57 million Uber accounts (3) the 145.5 million consumer data records on Equifax and (4) *every* Yahoo account – that's 3 billion in all! These very public data mishaps are causing consumers to question both the accuracy of digital information as well as the security of their own information stored digitally.

You would think that new technology developments would improve the situation. But in many cases, technology advances actually contribute to the problem. For example, an unsecured Internet of Things (more on this below) can become a ticking time bomb in the hands of hackers, causing loss of life and destruction of assets, as hackers use this information to misrepresent and blackmail people.

An even bleaker prediction--the technology research company, Gartner, predicts that by 2020 artificial intelligence (AI)-driven creation of "counterfeit reality," or fake content, will outpace AI's ability to detect it, tipping the scales in the direction of digital *distrust*. By 2022, Gartner predicts that the majority of individuals in mature economies will consume more false information than true information. Think of the potential impact that this could have on our economy, the political climate, and our society in general. The recent 2016 election fake news scandal could be just the tip of the iceberg.

Despite growing global distrust, people are becoming increasingly dependent on digital technology. In spite of security concerns, interestingly, people don't behave as if they mistrust technology. Instead, technology tools are being used more extensively in all aspects of daily life. The Fletcher School at Tufts University published a report in July 2017 confirming that this paradox is a global phenomenon.

To understand **Digital Trust** and what is required to implement this **TRUST**, it is important to evaluate the current state of the digital landscape.

2 IT Framework & Principles

“Addressing fundamental design issues”

IT Framework & Principles

The current IT framework has evolved based on the technical constraints of the time period, resulting in an unwritten model that guides our thinking and the development and deployment of existing and new technology. The way we apply the framework has changed over time, but the fundamental design issues have never been addressed. The following factors impact the framework and its long-term viability:

- **Silos of Data:** Lack of connectivity made it impossible to share data between organisations. The only way to use the IT framework was to duplicate the data wherever required; this silo-based framework is still in use today. People and objects are uniquely identified in every silo application. Silo data resulted in different versions of the **same data about people and objects identified by different identities** resulting in overall **low data integrity**.

- **Securing the data** was initially not a priority as no, or very little connectivity existed. As connectivity and the internet evolved, problems with securing data and keeping it private gradually became more problematic. **Security has never been part of the design of the framework and is therefore reactive**.

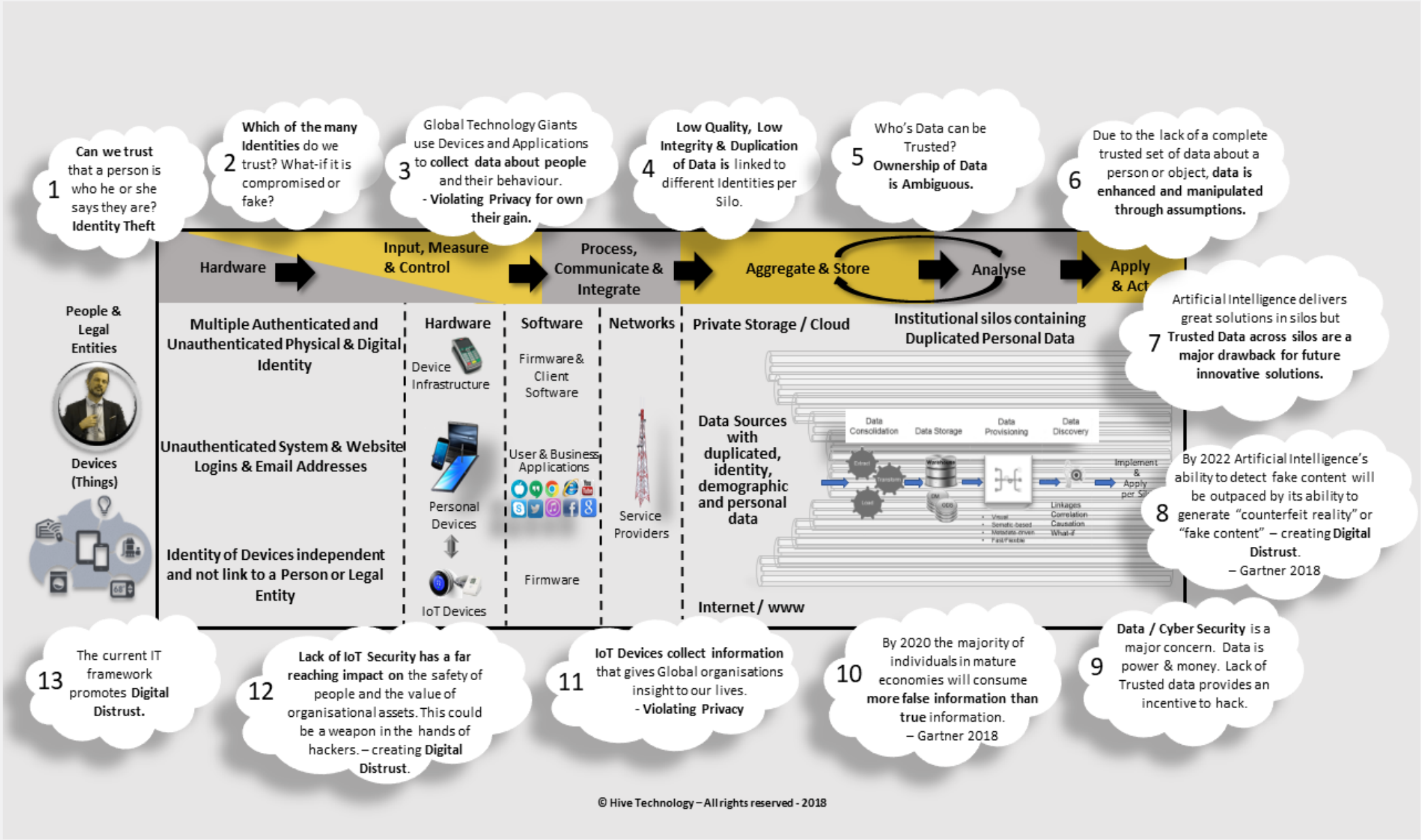
- **Ownership of data is ambiguous** and allows any company or individual that collect people's private data, to own, distribute, sell and manage the data. The actual data owner has very little, or no say regarding how the data is used, resulting in **deterioration of privacy** and **low-quality data** everywhere.

- **Big Data** and the combination of data from various sources and versions for analytics complicate this, resulting in massive amounts of data that is only partially correct, and, in some cases, completely incorrect due to the use of identifiers that are not unique--resulting in **low data integrity**.

- **Lack of a single authenticated identity** allowing **false, fake, duplicated and stolen identities** is the biggest problem in the current IT Framework. The reality is that data about people, objects and information is created in different silo environments and the Internet using various identities, mostly unauthenticated. These identities are not linked to any trusted identity such as a national identity issued by the government. The only industries that link trusted identity to their own identities are financial services and telecommunication, as this is required for governance reporting mandated by various internationally agreed statutes.

The diagram on the next page: **Digital Distrust in the current IT Framework**, highlight thirteen issues with the current IT Framework.

Digital Distrust in the current IT Framework



3 IT Framework & the Internet

“Lack of trust through the internet”

IT Framework & The Internet

The Internet uses the same IT framework to regulate the extension of the silos on a network and to websites, resulting in a myriad of sites and mobile applications all duplicating data. This has complicated the issue of digital trust.

The identities used on these sites and applications are created at registration and normally consist of a login, email address or mobile number and password, allowing anonymity as a fundamental reality of the online experience today. Because of this, site owners introduce friction such as CAPTCHAs, email, SMS, and phone verification. Although well intended, these deter legitimate users and not malicious ones. As a result, it is well known that fake accounts exist on all platforms, especially social media applications. In fact, Facebook and Twitter have publicly reported that the likely range of fake social accounts has historically been anywhere from 15-25%.

Due to the lack of trusted identity on the internet, it is safe to assume that fake users are responsible for a large amount of fake and unverifiable content. According to a new global poll conducted in 18 countries for the BBC World Service, 79% of the internet users surveyed worried about what is real or fake on the internet.

Internet of Things (IoT)

The Internet of Things is also an extension of the IT framework. We now allow devices to collect data and, in some cases, control actions via the internet while trusting manufacturers of these devices with our data and the related security. Opening accounts on IoT sites or applications uses the same identification methods as with the Internet and introduces the same problems.

We are trusting technology companies with our data, our assets and, sadly, many other aspects of our lives. SMART connected devices are one of the applications for IoT technology. With more than 3 billion Smart Phones, and other smart devices including appliances, personal digital assistants, and GPS engines all collecting data about behavior, preferences, and location, the issue of personal privacy looms large. And it isn't going to get any better. Next generation SMART devices will collect even more data about our behavior and detailed personal information about our daily activities. For example, toys that study our children will report play habits back to marketers. Consoles and home security systems will give corporations a window into our private lives, while connected medical devices will have the ability to provide data about our health and lifestyle.

4 Who is benefitting?

“Technology firms monitoring your every move”

Who Benefits?

The **Big Technology Companies** in the early 2000's realized the value of data. The big four technology companies in the US (Apple, Google, Facebook, and Amazon) are all built around collecting as much data as possible about people. Profiling people results in better free services and targeted advertising, which is the main source of income for Google and Facebook. Apple collects the same data, focusing on adding value to their very profitable technology devices. Amazon, on the other hand, focuses on the online shopping marketplace, with Alexa, an online voice recognition device, attempting to make an online order as simple as a voice command.

The reality is that the big technology firms can be seen as **"Big brother"** monitoring you and your every move, aggregating information to build a complete digital profile of you. Thousands of **"little brothers,"** the smaller companies and individuals try to benefit from data too, hacking and collecting as much data about you as possible-- to be bought, sold or stolen in an instant.
Most devices and software come with disclaimers, terms, and conditions protecting the technology companies. Users of these devices normally accept these terms and conditions without question, since we all know that it is the only way to obtain usage of these devices/applications. Most people don't even read the long, complicated legal documents attached and as a result, give away any rights they might still have.

U.S. residents already spend 10 hours a day using technology while 1 in 5 Americans say they are online "almost constantly." The tech companies have enormous reach and power. More than 2 billion people use Facebook every month. Ninety percent of search queries worldwide go through Google. Android is used in more than 2 billion devices and Apple IoS in more than 1 billion devices.

This results in enormous wealth for these companies. The top six companies in the world **worth more than $500 billion (source)** are technology firms. With more than **50% of the world population not on the internet (source)** yet and new emerging technologies, the power of the industry is only likely to grow.

5 Government

“Big businesses know more about you than governments”

Government vs. Enterprise

Technology and the global businesses that own the technology have become so powerful that they can disrupt and, in some cases, marginalize governments if governments don't respond quickly to this threat.

It is safe to say that technology companies know more about citizens than the governments of the countries they live and work in. The government may have access to static data, but dynamic data about behavioral preferences, interests, concerns, and beliefs --just a few of the factors that influence decisions and actions-- is available from the analysis and profiling that technology companies do. Information about societies and communities, social groups, and the cohesiveness of these groups can easily be obtained when groups of people are analyzed. The data used is not only the declared social media relationships, but a wealth of knowledge that can be obtained about people through location data collected on a minute by minute basis on smartphones.

Imagine the risk to national security when 3rd parties are able to influence citizens and communities in a country. Russia was able to impact the 2016 election campaign in the US through Facebook, Google, and Twitter. This phenomenon has raised concerns about whether the openness and reach of digital media is a threat to the functioning of democracies.
The evolving digital economy is not dependant on currencies, physical borders, or even trade agreements between countries and, for this reason, governments should get involved now.

Historically, global governments respond to threats through increased legislation rather than hands-on involvement. The first significant legislation, designed to protect citizen privacy and deal with some of the threats discussed, is the European Union's GDPR (Global Data Protection Regulation) that will give the **choice of who uses the data** back to the person whose data it is. Implementing legislation in the current IT Framework is virtually impossible and very difficult to police.

Governments are the only entities that have the power as custodians, with the citizens that vote for them, to change the IT Framework that underpins the future global digital economy and society. This requires hands-on involvement that we discuss later in this document.

6 Conclusion

“Changing Digital Distrust to DIGITAL TRUST”

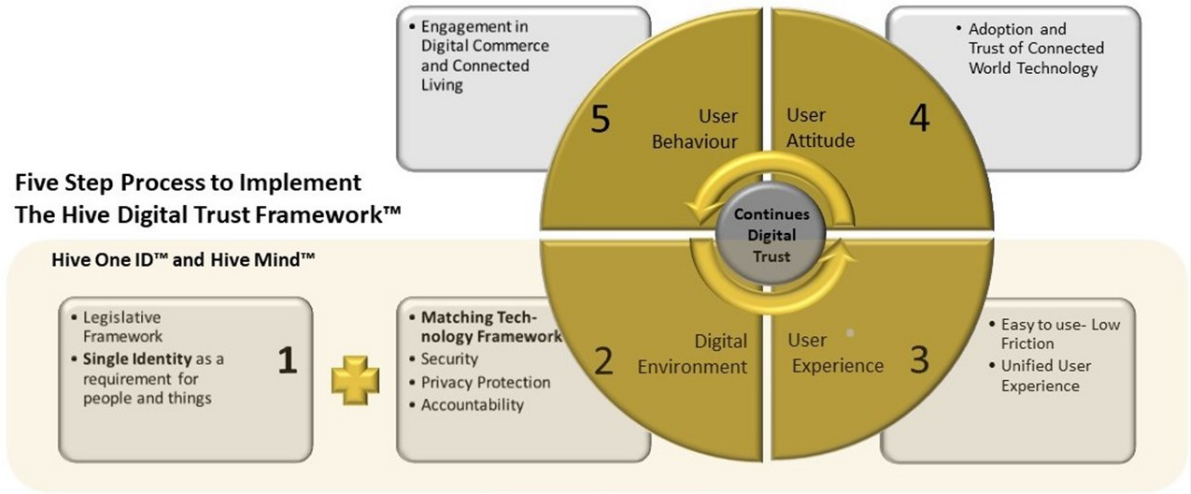
Creating Digital Trust

Even after analyzing and understanding the IT Framework and the different factors that contribute to Digital Distrust, it still seems virtually impossible to change the current technology landscape into one that can be Digitally Trusted. As the boundaries of the digital world expand, and more people become familiar with internet technologies and systems, their distrust will grow.

Some of the big consulting houses have published their views on Digital Trust. They believe that the answer lies in building a trusted digital solution between organizations and their stakeholders. As a result, companies seeking consumer trust will need to invest in becoming more trustworthy more widely around the globe. Those that do will likely see a competitive advantage, winning increased customer loyalty, enabling them to prosper in the digital era. The irony is that in doing so, the bigger Digital Trust issue will not be resolved, but rather will strengthen the silo mentality of the current IT Framework creating a new type of digital divide.

The real solution starts with governments. Governments, as the representative of the citizens of a country, must get involved in a very structured way to deal with Digital Distrust. The involvement of governments under no circumstances suggests that governments start to play the "big brother", but rather that they facilitate the creation of a legislative framework with practical building blocks that will secure the data of citizens and introduce a digital system that can be trusted. In so doing, they will create *a Digitally Trusted Economy that allows citizens to prosper in the Digital Era.*

Below, is the **Hiving Technology Digital Trust Framework.** It can be used to look at the steps required to build a digitally trusted country and economy. Building Digital Trust is a process and will not happen overnight, but can be built over time with the appropriate building blocks.



Hiving Digital Trust Framework™ Implementation

Step 1 describes the government's role as follows:
Provide legislation similar to the European Union's Global Data Protection Regulations protect citizens and resident's right to privacy and security.
Provide a single physical, and digital identity called a Hive One ID™ that can be used to identify and authenticate the citizen in both physical and digital interactions. The identity will point to the unique trusted set of data about the person or legal entity and will facilitate all identity requirements over time.
Implement requirements for trusted identities on IoT devices that collect data about people or legal entities.

Step 2 ideally will be provided by a PPP (Public Private Partnership) between Hiving Technology and the government:
Provide the infrastructure and matching information technology framework required to host a set of trusted data about every citizen and legal entity in the country, owned, managed and uniquely encrypted by the citizen or legal entity. IoT device identities link these devices to owners. The framework ensures data security, privacy, and accountability. From here trusted data can be provided on a permission basis to whichever 3rd party requires it.
Align government systems to use, share and update data owned by citizens and legal entities that are relevant to governing a country.

Step 3 ensures ease of use and low friction user interactions. These application plugins are developed by the developer community at large, using certified application development tools. The applications are automatically opened on the person's phone when the person is identified at a specific location. Services thus follow the person automatically but only activate and share data on permission from the owner of the data.

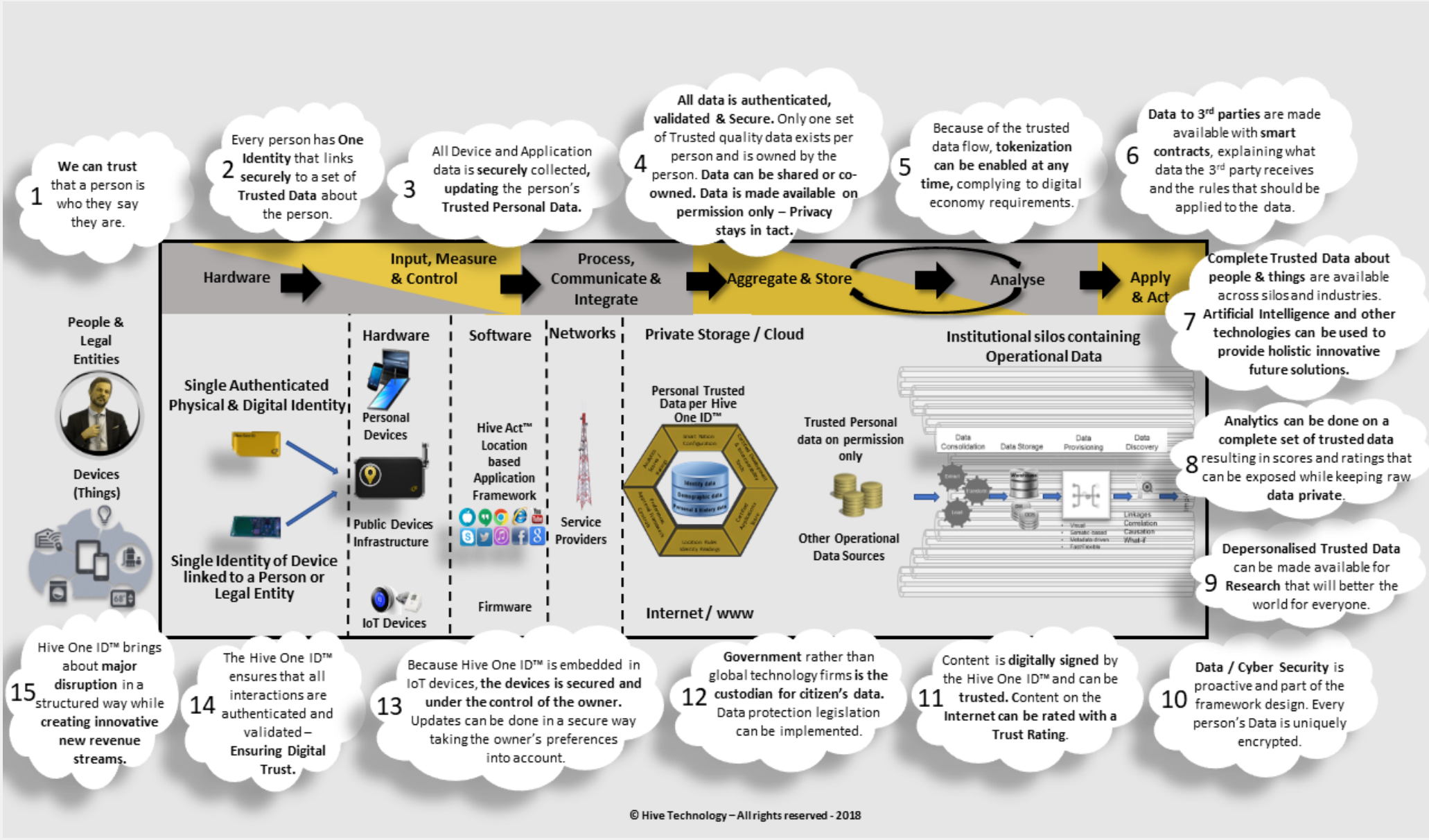
Step 4 automatically happens when users **trust** the technology and feel they are in control of sharing data to obtain services.

Step 5 now that people/citizens **trust** the technology delivering the services they will be likely to employ the technology in more aspects of their lives building a strong digital economy.

The Hiving Technology Digital Trust Framework™ can be deployed in the same way in countries across the globe, retaining local autonomy while seamlessly integrating into a global digital world. As inequality disappears – more people have an opportunity to participate in the trusted digital world. In less-trustworthy countries who choose not to participate, users will need governments to enact strong digital policies to protect people from fraudulent scams and fake information, as well as regulatory oversight to protect consumers' data privacy and human rights, all very difficult to accomplish effectively.

The diagram on the next page: **The Hive Digital Trust IT Framework**, highlight fifteen strengths achieved on implementation of the framework.

The Hive Digital Trust IT Framework



7 Third Party Review

Clabby Analytics

Clabby Analytics

www.clabbyanalytics.com

Some of the biggest advancements in technology today are fueled by data. The Internet of Things, Artificial Intelligence, Augmented & Virtual Reality, SMART devices and Big Data Analytics are all driven by data – all different kinds of data including machine data, social media data, transactional data and personal data. With this data, we can do all kinds of things. From paying bills to personalized shopping to driving automated SMART cars, data is at the core.

What is not highlighted is what happens when this data is incorrect, tampered with, compromised or gets in the wrong hands. Today various versions of our personal data exist, depending on how accurately it was collected or deducted, who gathered the data, and when it was collected. With new technology advancements, we not only have to **trust** the technology, but also **trust** that the data used to drive this evolving intelligence is correct. It is safe to say that **DIGITAL TRUST** is the key factor in the transition to a Digital Era.

Clabby Analytics recently attended a seminar on Smarter Cities in Dubai, UAE where we had the pleasure of meeting and introducing Gert Botha, CEO of Hiving Technology. Upon further discussion, we discovered our companies have a similar interest in Digital Trust. With data scandals like Facebook & Cambridge Analytica, or data breaches like that of Equifax, Clabby Analytics has taken a strong stance on data protection and security. After learning about the Hiving Technology approach, it is obvious to us that fundamental change is required.

There are two problems that need to be addressed in the transition to the digital world. First, *a single identity for objects and people is no longer negotiable*. Second, in order to trust the data powering the new generation of technologies*, it must come from a single trusted source linked to a single identity*. The question is how to achieve this in a market where there are more new identity products launched rather than a consolidation of existing products. The other issue is that ownership of data is now seen as an asset to organizations.

Hiving Technology, and their Hive Digital Trust Framework have the only solution we have come across thus far. The solution consists of a single identity called Hive One ID linked to a set of trusted data, managed by a set of utilities called Hive Mind. Clabby Analytics and Hiving Technology believe it is important to outline why there are weaknesses pertaining to Digital Trust in today's IT Framework, and how to approach those weaknesses and fix them.

The eBook by Hiving Technology describes, in detail, the issue of Digital Trust and more importantly, how our current IT Framework has resulted in a culture of Digital *Distrust.* It also introduces some unique and valuable insights, and a step-by-step process for businesses and governments to restore Digital Trust.

Learn more about how Hiving Technologies is changing digital trust

www.hiving.technology

Contact us

Gert Botha: +971 55 391 5313
E-mail: info@hiving.solutions