

van den Dam, Rob

Conference Paper

The trust factor in the digital economy: Why privacy and security is fundamental for successful ecosystems

14th Asia-Pacific Regional Conference of the International Telecommunications Society (ITS): "Mapping ICT into Transformation for the Next Information Society", Kyoto, Japan, 24th-27th June, 2017

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: van den Dam, Rob (2017) : The trust factor in the digital economy: Why privacy and security is fundamental for successful ecosystems, 14th Asia-Pacific Regional Conference of the International Telecommunications Society (ITS): "Mapping ICT into Transformation for the Next Information Society", Kyoto, Japan, 24th-27th June, 2017, International Telecommunications Society (ITS), Calgary

This Version is available at:

<https://hdl.handle.net/10419/168536>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

The trust factor in the digital economy – why privacy and security is fundamental for successful ecosystems

Rob van den Dam

IBM Institute for Business Value

Rob_vandendam@nl.ibm.com

Abstract

The volume of personal data collected by organizations is considerable and growing. But as more data is collected and transacted, the likelihood of a breach escalates. Cyberattacks are increasingly common and the volume and severity of data breaches and abuse continue to increase. With more and larger breaches in the news, consumers have become worried about – and suspicious of – the organizations that collect, store and use their data. And as digital ecosystems and the Internet of Things further expand, protecting customer data is more urgent than ever before.

1. Introduction

Personal data is the new currency of the digital economy. Generating insight from personal data can bring tremendous benefits to both individuals and organizations, and to society as a whole. But at ever-increasing risk. Cyberattacks, data hacking and surveillance practices make consumers uneasy about the privacy and security of their personal information.

Trust in the organizations that collect and maintain personal data is decreasing, particularly in mature markets. Consumers are caught in the middle between organizations that need (or want) their data for mutual benefit and malicious forces that want to steal it. Customers say they want more personalized experiences. But for this to work, enormous amounts of personal information must be gathered, analyzed and secured. This is where trust can become a game changer.

The volume of personal data collected by organizations is considerable and growing. In addition to official records, demographic data and information voluntarily provided, people also, often unknowingly, leave digital footprints – browsing history, location data, social media activities, online purchases and more. Increasingly, data collected from smart devices and the IoT are becoming part of this footprint. For example, navigation apps can show where a person has traveled. Connected cars reveal driving habits. Smart utilities can record the activities of a person at home. [1]

For organizations and consumers, there is tremendous value in the ability to aggregate and analyze all this personal data and, most important, be able to create insights that enable its profitable use. (see Figure 1).

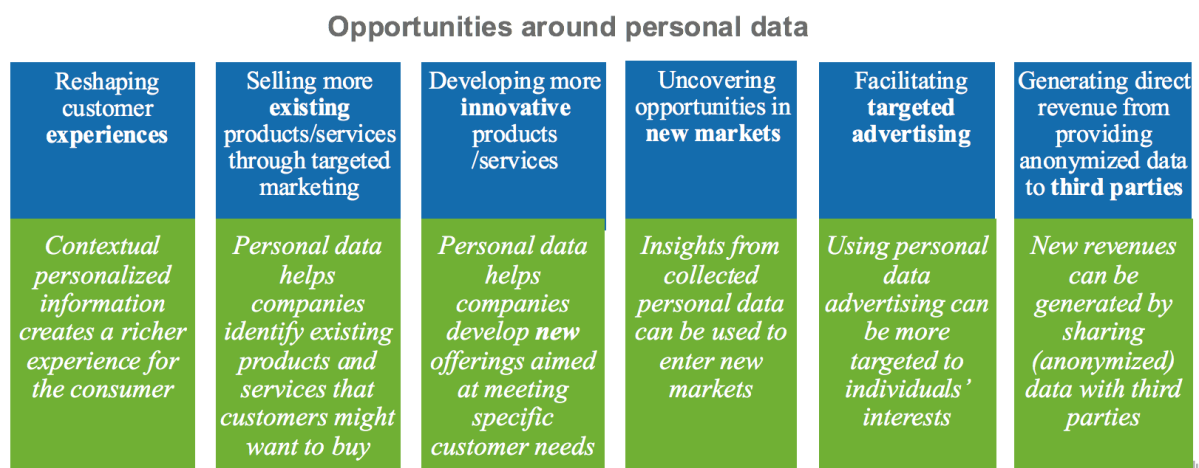


Fig. 1. Tremendous untapped value lies in the ability to aggregate and analyze personal data

Monetizing personal data has become the new battleground, something the Internet platform companies – such as Google, Facebook, Amazon and Alibaba - clearly understand. These companies maintain huge repositories of customer data, often generated by consumers when they visit their web sites. The importance of data is illustrated by the large sums paid to acquire organizations that maintain vast amounts of personal information, such as WhatsApp, bought by Facebook, and LinkedIn, purchased by Microsoft.

2. Sharing personal data vs. privacy

Smart devices are increasingly used to harvest huge amounts of personal information. However, at the same time, hackers have an extended surface area and potential to completely disturb society by abusing personal data stored on connected devices. And as more data is collected and transacted, the likelihood of a breach escalates. Cyberattacks are increasingly commonplace, fueling consumers with unease about the privacy and security of their personal information. And as digital ecosystems and the IoT further expand, protecting customer data is more urgent than ever before. [2]

Media frequently report about companies, institutions – and even governments – abusing personal data. The volume and severity of data breaches and abuse continue to increase. Though personal data is a central ingredient in scaling up ecosystems and the IoT, privacy and security issues are real sources of concern for consumers, society and regulators:

- Consumers might reach a tolerance level threshold for their trust in sharing personal data
- Ecosystems occupied by the IoT - which would include data streams from connected cars, smart cities and the like – might be impacted by cyberattacks
- Regulators, being keenly aware of the risk for public safety and personal data protection, might see arguments for limiting the confidentiality of the data being exchanged.

Consumers have become worried about – and suspicious of – the organizations that collect, store and use their data. To identify the factors that influence trust, as well as to develop insights that can help ecosystem players capitalize on it, we surveyed nearly 21,000 consumers in 42 countries to access consumer mindsets and trust imperatives related to privacy and security. [3]

In emerging markets, communications service providers (CSPs) are the most trusted organizations by consumers for handling personal data. In mature markets, CSPs are

second only to banks/credit card companies. At the bottom in trust in mature economies are social media companies such as Facebook. (see Figure 2).

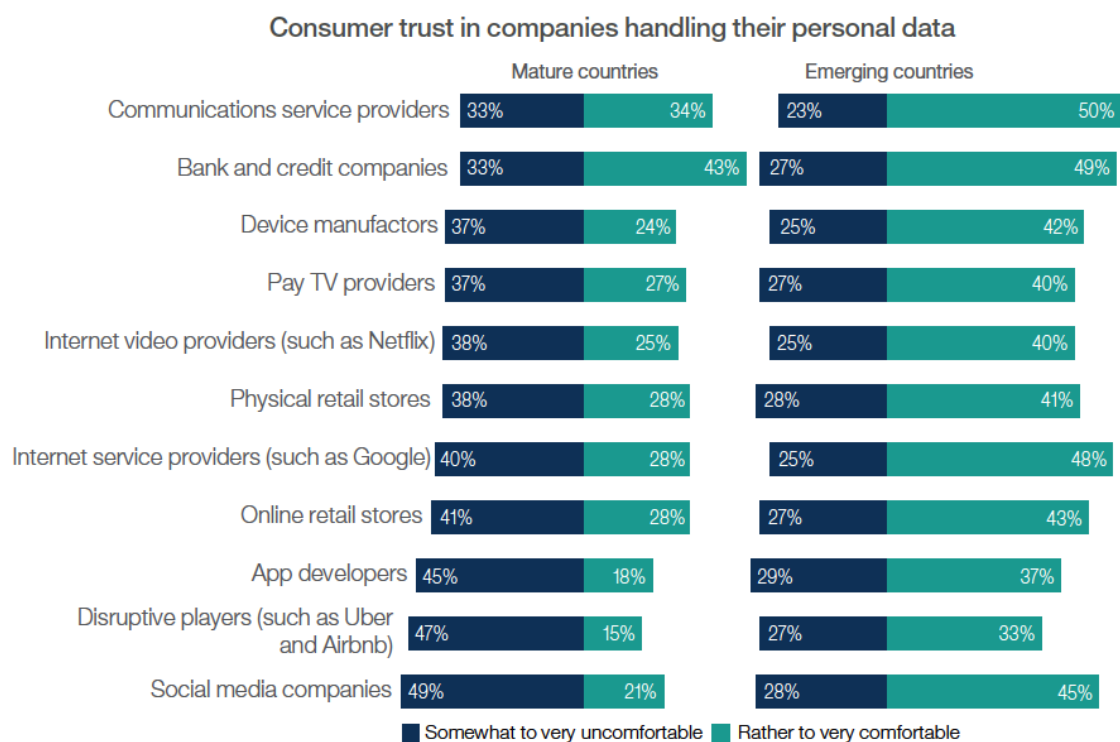


Fig. 2. Consumer trust in companies handling their personal data

Of course, the notion of trust in organizations further varies across individual countries. For instance, in Greece and Italy, consumers rate CSPs significantly above banks, while in such countries as Egypt, Saudi Arabia, Indonesia, Philippines and Thailand, internet service providers (such as Google) and social media companies are first and second, above CSPs.

Trust varies by age as well. Globally, 40 percent of consumers in the 18-25 age group in our survey indicated they feel comfortable sharing personal data with their CSPs. For the 26-45 group, the number grows to 44 percent. However, only 33 percent of those over 45 said they trust their providers.

Over the past three years, trust has declined across the board for all organizations that handle personal data (see Figure 3). The primary concern of consumers (60 percent in our survey) is that organizations might sell their personal data to third parties without their consent. Forty-five percent were concerned their data might not be secure, and 35 percent were concerned about how much these companies knew about them.

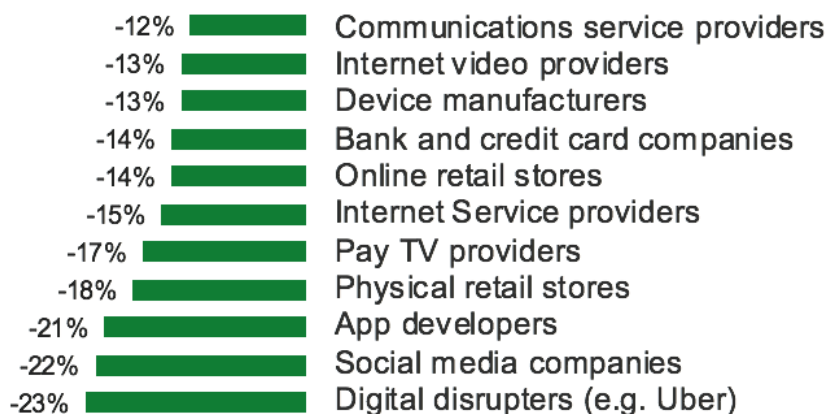


Fig. 3. Decrease in consumer trust in organizations in the last 3 years

3. Trust: the battleground for competitive advantage

Gaining – and keeping – digital trust is the prerequisite for any organization that wants to capitalize on personal data to create value. Trust in a company gives customers the feeling their data is in safe and secure hands and increases willingness to share information, even if just minimal value is offered in return. Further, trust motivates spending and loyalty and enables the organization to offer more relevant revenue-generating services and applications.

Consumers, according to their answers in our survey, can be segmented into three distinct trust mindsets according to their perceptions and actions about data sharing. These mindsets reflect how willing consumers are to share data and whether they take defensive actions to avoid giving away personal information:

- Consistently trustful – This group is alarmed, but not frightened. They understand the seriousness of data breaches, but do not believe the situation is as bad as media coverage implies. This group tends to be a bit lax in protecting against

abuse of personal data.

- Increasingly suspicious – This segment is very suspicious about how organisations handle personal data and are not certain the data can (or will) be kept secure. Increasing media attention to data hacks and cyberattacks result in even less trust. This group goes to significant length to protect access to data, such as deleting or blocking cookies and using different web browsers.
- Trustful-but-worried – This group is the most positive about how they can benefit from sharing data. They have a high trust in organizations in general, and this trust continues to grow. They say they benefit from data sharing by getting better services, products or experiences. However, they worry about how the organizations handle their data and are concerned that they will sell their data to third parties. As a result, they try to control access to their personal data as much as possible.

Each of these segments takes a different view about the relative importance of the three pillars upon which digital trust is built: transparency, value exchange and security. Organizations must evaluate how the different mindsets value these trust attributes and respond accordingly. Understanding the yin and yang of customer mindsets and trust imperatives is the key to increasing trust and subsequent improvement in monetization opportunity (see Figure 4).

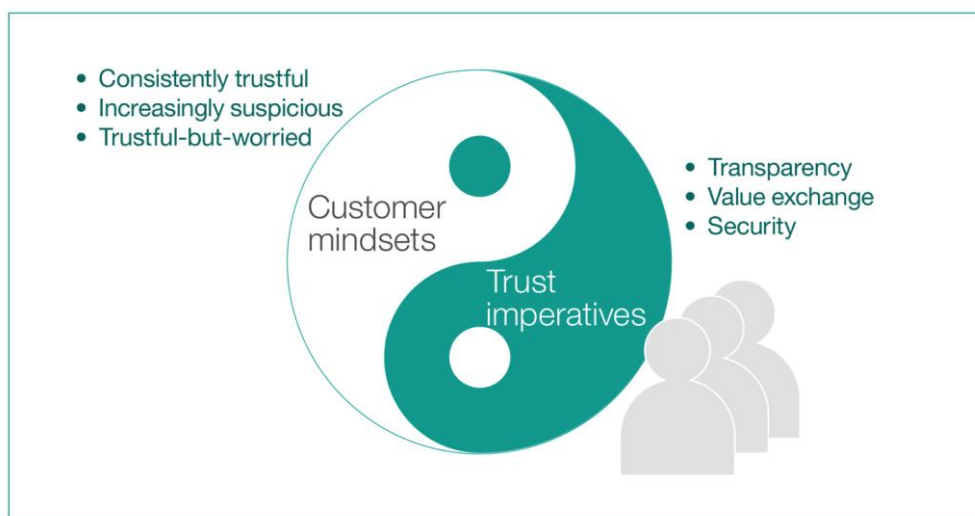


Fig. 4. Organizations need to manage the yin and yang of customer mindsets and trust imperative

4. The three imperatives of trust

(a) Transparency

Most of the respondents to our survey have only limited knowledge about what types of personal data are collected and how it is used. Further, 64 percent of respondents indicated that finding out what data is collected and used is at least moderately difficult.

With such difficulty, it should come as no surprise that respondents cited transparency as the top driver in building trust (see Figure 5). Customers want to know how their data is used and by whom.

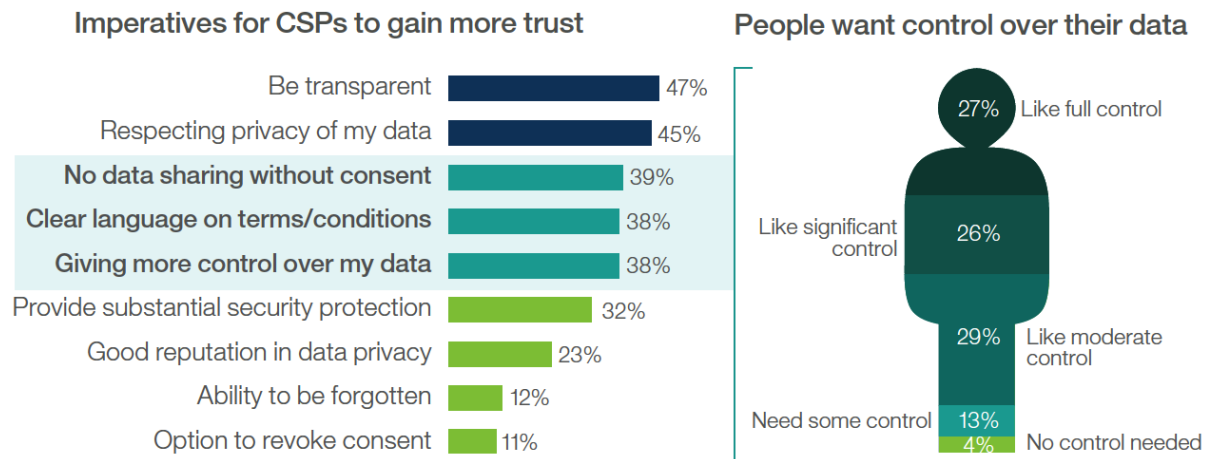


Fig. 5. Transparency and privacy are the two primary drivers to build trust. People also want more control over their data

Consumers in our survey said it is important that providers tell them what personal data is collected and how it is stored and used. However, there were some differences among the three customer mindsets, with 45 percent of the increasingly suspicious, but only 29 percent of the consistently trustful, saying this is extremely important to them. In addition, the sense of having no control over their data is one of consumers' growing concerns. Fifty-three percent of overall respondents say they would like significant-to-full control over the data they share, possibly using a browser or an app. They want control over whom they share data with, how they share it, as well as what they get in return.

(b) Value exchange

Offering a fair value in exchange for personal information, and making the exchange transparent, is a key element in building trust. A mutually beneficial arrangement allows businesses to gain data they (or third parties) can use to better understand, service and/or target consumers. In return, the customer should receive something of value, such as superior service or a financial reward. However, consumers say they are often not adequately rewarded for use of their personal data. [4]

Consumers value personal data based on the type of data and how it is used. Data held by commercial organizations and institutions (such as banks and healthcare organizations), as well as digital footprints, are considered most sensitive. Consumers require more return value to share these types of information. To facilitate willingness to share personal information, individuals must understand how they benefit from it. Examples are:

- Improved service or experience – Consumers generally feel the enhancement itself is a fair trade for their data
- Free or discounted products/services
- Recommendations for products, apps, content and services
- Targeted offers or advertising – Many consumers do not see this as a value exchange and would rather avoid advertising messages
- Part of the value from selling to third parties – In general, consumers will expect more value in return for personal data sold to third parties
- Compensation in other forms – Many consumers just want a reward in the form of a discount, cash back or a coupon.

(c) Security

Cyberattacks are becoming increasingly common and often make headlines. Consider, for example, just a few from 2016: data stolen from a billion Yahoo customers, Caller ID apps exposing 3 billion names and numbers from users, stolen customer records (from Verizon) even put up for sale and more.

Consumers are increasingly concerned about the protection of their data, and it is vital to organizations for them to know how security is guaranteed. This is particularly true for both older customers and those of the suspicious mindset in our survey, with 50 and 54 percent of them, respectively, indicating knowledge of data security is very critical (see Figure 6).

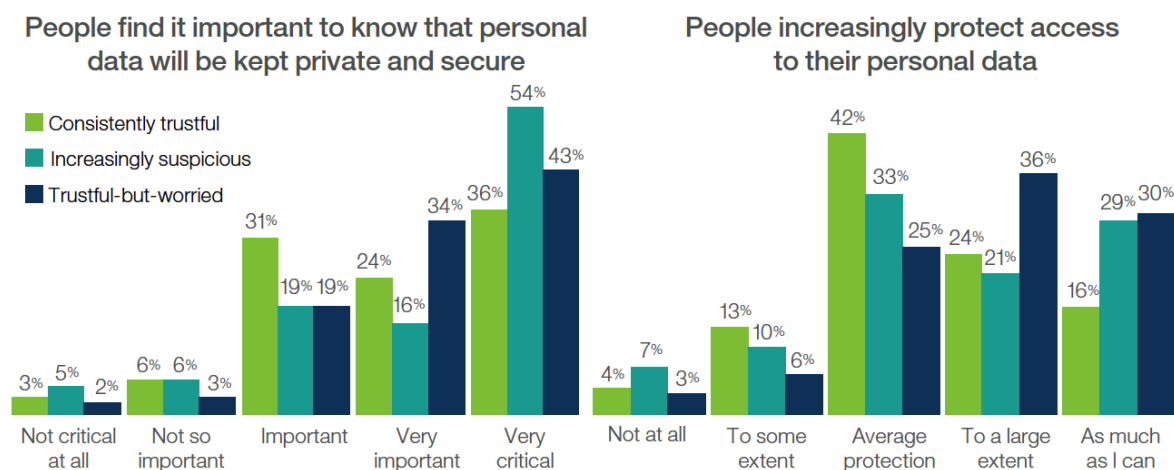


Fig. 6. More suspicious customers need to know that organizations keep their personal data private and secure; they also protect access to their data

Most consumers surveyed said they believe many organizations misuse their personal data on the Internet, and many have taken protection measures themselves, blocking cookies, using different browsers, opting out where possible and using advanced online tools.

5. Technologies

Organizations should focus on developing technologies – such as cognitive computing and block chain technology - necessary to develop actionable insight from the huge amount of personal data and to establish transparent, private and secure environments.

Cognitive computing technology

Personal data is vast, diverse, complex and continuously changing. Most data is unstructured and invisible, such as that hidden in videos and sensors. Traditional analytics cannot fully extract the value of this data. Cognitive computing technology is a key enabler to unlock the full value of unstructured data, which accounts for about 85 percent of all data generated. [5]

Cognitive computing technology provides more *detailed insights* from personal data than traditional analytics solution can deliver and creates increased value for both customers and organizations. Cognitive systems can:

- Handle large volumes of both structured and unstructured data
- Learn actively from things, context, and the way people interact with them
- Adapt and evolves to be more useful and robust over time
- Relate insights in easily understandable ways, such as natural language/dialog, text and visual cues.

Cognitive technology can also be used to *identify security threats*. Cognitive security systems are then deployed to analyze vast amounts of structured and unstructured data to provide insights into emerging threats, as well as recommendations on how to stop them.

Block chain technology

The Internet was originally built on trust, but all the data breaches and cyberattacks have made that a thing of the past. With the ever-expanding IoT, it is more important than ever to secure personal data handling and privacy. It is key to move from a “security-through-obscurity” (closed source) approach to one that is based on transparency. Blockchain offers a potential solution by enabling private and secure personal data handling. [6]

The blockchain is a decentralized public ledger of transactions that no one person or company owns or controls. In addition, the technology can secure a company’s network by placing the identities of all authorized users in the blockchain ledger, which

continuously verifies them. As a result, it is better able to withstand malicious intrusions and provide users control of all their information and transactions. The technology also allows for ecosystem simplification.

6. Concluding remarks

Digital trust has become a key factor in the depth of relationship between consumers and organizations. Recent well-publicized data hacks and security breaches have humbled even mighty companies, leaving their reputations in question and their balance sheets damaged. Customers feel violated and deceived when their personal data is compromised. Once trust is lost, it is nearly impossible to regain. When such brands fall out of public favour, their value also decreases significantly to potential ecosystem partners.

To increase trust levels, as well as the resulting potential revenue opportunities, organizations need to understand the various levels of trust consumers place in organizations, as well as the contributing factors that define trust: transparency, value exchange and security. This knowledge will allow organizations to develop initiatives and services that promote increased trust, identify partners that can help them deliver these services, and adopt the technologies necessary to establish transparent, private and secure environments.

Sources

- [1] Personal Data: the emergence of a new asset class, World Economic Forum, Jan, 2011
http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf
- [2] Overcoming the digital trust deficit, World Economic Forum, January 2015,
<https://www.weforum.org/agenda/2015/01/overcoming-the-digital-trust-deficit/>
- [3] Highlights from the fall 2016 Global Telecom Consumer survey, IBM, February 2017,
<https://www-935.ibm.com/services/us/gbs/thoughtleadership/2016telecomsurvey/>
- [4] The future of digital trust: A European study on the nature of consumer trust and personal data. Orange. February 2014.
<https://www.orange.com/en/content/download/21358/412063/version/5/file/Orange+Future+of+Digital+Trust+Report.pdf>

[5] Your cognitive future - How next-gen computing changes the way we live and work, IBM, January 2015,

<https://www-935.ibm.com/services/us/gbs/thoughtleadership/cognitivefuture/>

[6] “Fast forward: Rethinking enterprises, ecosystems and economies with blockchains.” IBM. June 2016.

<https://www935.ibm.com/services/us/gbs/thoughtleadership/blockchain/>