IMD
REAL LEARNING. REAL IMPACT

Strengthening Trust in Technology When it Matters the Most

ST.GALLEN SYMPOSIUM

CONTENTS

SPOTLIGHT FEATURE

How do we tackle digital's crisis of trust?

By Öykü Işık, IMD Professor of Digital Strategy and Cybersecurity

Public and private sector actors must work together to adopt existing tech solutions for the crisis in trust, while fostering platforms for stronger stakeholder engagement and building more robust frameworks for legislation and self-regulation.

There is a looming crisis of trust in digital technologies that threatens to derail progress and further infect cyberspace with society's problems.

Personal data can be stolen en masse or used well beyond the intentions of users. Governments struggle to regulate quickly enough to cope with the pace of change. Social media bots and deep fakes can distort reality and influence our world view. Unintended consequences can be triggered by companies or authorities that mean well. Vital systems are vulnerable to debilitating cyber attacks.

Of course, we all need the digital world, but what type of digital world do we want? For some, the abstract nature and language of digital technology is too complex to truly understand. For others, the growth of technology and data use raises serious questions about ethics and participation.

This has triggered an erosion in trust in an online domain that has so swiftly become a necessary pillar of daily lives.

Unless private and public sector organizations – and individuals – act now to resolve these challenges, this crisis of trust will only accelerate, with consequences for our economies, people and planet.

Urgent answers for urgent questions

Against this backdrop, the rapid adoption and innovation of digital during the COVID-19 pandemic has raised more questions about digital ethics, privacy and cyber security.

Without action, the digital transformation that is necessary for a fairer economic future and progress towards UN Sustainable Development Goals could prove elusive. There is also a danger that online users could lose faith in companies, governments, social media platforms – and each other, if we do not collectively invest in trust building initiatives.

How did we find ourselves on this boulevard of broken algorithms? Yes, we've all heard the stories about malware attacks and identity theft. But the challenges run far deeper and reflect broader societal issues.

Take Black model Joris Lechêne who, in April 2021, demonstrated how racial bias has become hardwired into official AI-powered passport application software in Britain. As part of his application, he was required to upload a portrait photo – and followed the guidelines correctly. His photo was rejected because the software could not accurately recognize his features.

> "From an ethical, economical, technological and legal viewpoint, rebuilding trust in digital is critical for business, sustainability and security."

AI can help us reach **134** UN SDG targets

AI can hinder **59** UN SDG targets [1]

You may have also heard about the controversy over Amazon's Ring. It has recently come under scrutiny over questions about the way home security footage is shared with law enforcement and how the biases of police officers might impact the rights of vulnerable communities.

So, the crisis in digital trust is not just cyber attacks or awkwardly targeted online ads – it's about society's problems becoming irreversibly embedded in the online world. Joris' experience shows us just how vulnerable technology remains a long way from being robust.

It is hardly surprising that we see growing negative sentiment towards corporate and government actors when it comes to their data collection and processing initiatives.

Data protection regulations, such as the EU's GDPR, have forced organizations to be more transparent, as well as targeted, in their consumer data collection activities. This has revealed several occasions where organizations' data collection and processing justification was not only far from ideal, but deceptive. In 2019, Google was fined €50 million for the way it processed data for the personalization of ads.

Why is it so important to tackle this problem now?

Digital ethics challenges are already shaping our present and will determine our future social and economic interactions. Digital technologies have enormous economic potential and are critical in reaching the UN Sustainable Development Goals (SDGs).

Let's take AI, for instance.

AI, as one of the most heavily invested-in technology families, can be used to process remote sensor data to contribute to environmental protection or optimize energy distribution, for example. In fact, recent research suggests that AI can support progress towards more than 130 of the 169 SDG targets. Crucially, the same investigation estimated AI could also become a hinderance to almost 60 of those targets.

The use of AI can also have tangible negative impacts in everyday lives. In the Netherlands, 26,000 families were falsely accused of cheating the child welfare system, in part because of a discriminatory algorithm. This led to the resignation of Prime Minister Mark Rutte and his entire cabinet.

These examples underline the complexity of the challenges that we face. Even when technology is "for our own good", issues of trust remain. When technology is adopted as quickly as during the COVID-19 pandemic, we become part of the experiment – prone to all the mistakes that can happen when regulation lags behind innovation or development processes are imperfect.

90% of the Leaders of Tomorrow say fake news frequently circulates on social media [2]

Even the development of COVID-19 tracing apps – a crucial tool in helping to save lives and end the pandemic – has fallen foul of the crisis of trust.

Some saw these tracing tools as intrusive and complained about a lack of transparency about the use of data collected. Singapore's app proved popular at first, with the promise that data would only be accessed if a user tested positive for the virus. However, trust in the app suffered after it was revealed that law enforcement could access data for their investigations.

From an ethical, economical, technological and legal viewpoint, rebuilding trust in digital is critical for business, sustainability and security. But, once trust is lost, it is difficult to regain. It follows, therefore, that the public and private sector must double down on finding effective solutions to rebuild trust before it is too late.

Four building blocks that demand attention

In this white paper, based on discussions during the 50th St. Gallen Symposium, on "Trust Matters" (5-7 May 2021), we explore ways to stave off the looming crisis of trust in poorly understood digital technologies and the organizations that use them.

Our discussions, drawing on expertise from big tech companies, other private sector voices, academia, next generation leaders and public sector organizations, focused on sharing viewpoints and possible solutions across four building blocks for the future of data, against the backdrop of COVID-19: individual, technological, organizational and societal.

In this paper, we summarize these insights to inform the public debate around the complex trade-offs and challenges spanning these four interdependent blocks.

The roundtable and this paper did not seek to create consensus, but to give a platform to diverse opinions. As such, the summary recommendations put forth may not reflect the views of all participants.

One point was clear for all, however: Without a stronger level of cooperation and open dialogue between private and public sector actors, we are unlikely to find meaningful solutions and the crisis of trust could gain momentum.

We hope this paper proves to be a meaningful and insightful contribution to the debate around the search for solutions.

INTRODUCTION

Rebuilding public trust in the digital world

This white paper draws on expert recommendations and insights from the 50th St. Gallen Symposium to inform the search for solutions to the crisis of trust in the digital space.

The COVID-19 pandemic has demonstrated the potential of emerging digital technologies to contribute to solving the world's most intractable challenges. Information and communication technologies (ICTs), in particular, have allowed us to stay connected in times of physical distancing, to collaborate remotely, and to educate and learn despite school closings. What this has shown is that, when used in the right way, technology and digitization can be a force for good, and a central success factor in recovering from the pandemic quickly whilst addressing some of our most pressing challenges in the long term.

To reap this potential for positive impact, societal trust in emerging technologies, and those who develop and market them, is fundamental – but has been challenged in recent years. Trust in technology is diminishing at a time when we require it the most, with socioeconomic forces impacting technology as technology impacts them.

During the 50th St. Gallen Symposium on "Trust Matters", senior executives and a selected group of next generation leaders came together during a virtual roundtable to share their perspectives and discuss solutions to the most pressing digital trust challenges, curated by IMD Professor of Digital Strategy and Cybersecurity Öykü Işık.

The debate was guided by the following frame and questions:

The COVID-19 pandemic has underlined the potential to use the growing amounts of data we all produce to help us solve pressing problems. One of the many examples includes using AI for COVID-19 chest X-ray interpretation, to improve diagnosis precision and reliability. Moreover, at least 45 countries have developed their own COVID-tracing app. Yet, examples of collected data by these apps being used for unrelated purposes started surfacing quickly in some countries – ultimately eroding users' trust. This has brought up important questions about the right balance and relationship between privacy and data protection, on the one hand, and the quick rollout of innovative applications of ICTs and AI for our health and security, on the other. While paradigms such as privacy by design suggest that this does not have to be a zero-sum game, we do not yet see this by and large in action.

- What does data protection mean following the COVID-19 pandemic?
- What are trade-offs and synergies between privacy, and effective and swift problem-solving through innovative applications of ICTs, and how do we best manage them?

In order to address these issues of trust, the roundtable's participants suggested a range of approaches and solutions across the following four building blocks:

- **Individual** – personal tools, policies and responsibility
- **Technological** – finding and using effective technological solutions
- **Organizational** – companies taking steps to repair and build trust
- **Societal** – designing regulations and solving ethical questions

EXPERT RECOMMENDATIONS AND INSIGHTS

THE INDIVIDUAL CHALLENGE

- Individuals should be able to take more responsibility and be given greater powers to manage their own data
- More education is required to improve understanding about data risks, rights and available tools
- Individuals could demand and be given a right to review, not just delete, data
- Individuals could demand and be given a share of monetisation from data use

"Data governance should protect the powerless. We should move from data protection to data emancipation."

BENEDIKT SCHUPPLI
CO-FOUNDER AND CO-CEO, FQX

"Lifelong learning is key to make sure the digital divide does not deepen further but can begin to heal."

NINIANE PAEFFGEN
MANAGING DIRECTOR, SWISS DIGITAL INITIATIVE

"In addition to the right to delete, which is part of GDPR, we should have the right to review [...] There is a need to develop more robust systems to properly manage this monetization of data value accretion."

JEFFREY BOHN
SENIOR ADVISOR, SWISS RE INSTITUTE

THE TECHNOLOGICAL CHALLENGE

- Self-sovereign identity could be more widely adopted to establish trust in non-physical transactions and to reduce the excessive sharing of personal data
- Decentralized distributed ledgers, similar to technology used in blockchain, can improve transparency, cyber security and enhance trust between parties
- Homomorphic encryption and confidential compute can enable third-party processing of important data, such as health information, without compromising individual privacy
- AI systems and machine intelligence should be designed with privacy, ethics and security as built-in, not bolt-on

"We have to deploy and fix security by design from the very beginning. We need to rethink the tools. Having more decentralized tools, and not this centralised model, gives better transparency, but also a better way to avoid single points of failure, when we have data breaches."

KATERINA MITROKOTSA
PROFESSOR OF CYBERSECURITY, UNIVERSITY OF ST. GALLEN

"We need to spend more time in applying some of the new techniques coming out of confidential compute research ... If we require this of enterprises, we will massively reduce vulnerability."

JEFFREY BOHN
SENIOR ADVISOR, SWISS RE INSTITUTE

"We need to look deeply into what technology can do on confidential compute and encryption, but also look at something like a Hippocratic oath for developers."

MARIANNE JANIK
AREA VICE PRESIDENT, MICROSOFT GERMANY

THE ORGANIZATIONAL CHALLENGE

- Organizations have yet to embrace all the technological solutions and business practices available to improve trust
- Tech companies and social media platforms can do more to improve data management policies, transparency and build trust through education and effective self-regulation
- Companies should be ready to share the benefits of data with users
- The tech industry should consider a Hippocratic oath or code of conduct with implications for malpractice to improve quality and ethics of innovation

"Politics needs to set frameworks and conditions to make sure trust can grow, but business must also live up to its societal responsibility."

NINIANE PAEFFGEN
MANAGING DIRECTOR, SWISS DIGITAL INITIATIVE

"There is a lot that companies themselves can do to adopt practices and policies voluntarily. There are technological and legal and other innovations that can unlock valuable insights from data while protecting the interests of different stakeholders. Yet, they are still not adopted widely. You don't have to wait for regulation."

MANJU GEORGE
HEAD, STRATEGY, PLATFORM ON DIGITAL ECONOMY AND NEW VALUE CREATION, WORLD ECONOMIC FORUM

"We will need regulation and we need standards, but we really believe in the meantime in organizational accountability and shared responsibility."

SOPHIE BATAS
DIRECTOR FOR CYBER SECURITY AND DATA PRIVACY, HUAWEI

THE SOCIETAL CHALLENGE

- Society could consider shifting its focus from data protection to data empowerment and the adoption of a minimum required usage approach
- More dialogue and forums for collaboration are required to bridge gaps between public sector regulation and private sector innovation
- Existing data regulations need to be aligned, relevant and applied evenly across borders
- Authorities with investigation powers could be created to determine causes of data breaches or cyber attacks to avoid repeat future events

"GDPR was a great step forward for the European Union, but the problem for us is at a practical level every country in Europe implements GDPR differently, which creates legal uncertainty and makes it very difficult for young companies like mine with limited resources to navigate."

JONAS MUFF
CEO AND FOUNDER, VARA

"A lot of the promise of data can only be unlocked if it supports use cases across borders. We need policies and measures across borders that are compatible and interoperable."

MANJU GEORGE
HEAD, STRATEGY, PLATFORM ON DIGITAL ECONOMY AND NEW VALUE CREATION, WORLD ECONOMIC FORUM

"As soon as we see a good collaboration between public and private sectors, things can be solved effectively. The moment we have this bipolar world of public against private sector and we are looking to the public sector to solve these topics alone, it will not work. It takes at least two to tango."

MARCO HUWILER
COUNTRY MANAGING DIRECTOR SWITZERLAND, ACCENTURE

"How can we better manage and enhance this relationship and understanding between public sector governance and private sector innovation, so that countries and regions don't fall behind? How can we contribute to smart, effective regulation together?"

KULANI ABENDROTH-DIAS
STRATEGIC ANALYST, OECD

From exploitation to empowerment

Greater education and powers to control the destiny of our information online are needed to build a fit-for-purpose system of trust that individuals will commit to in the digital age.

Most individuals juggle a curious contradiction online.

We might be prepared to give up lots of personal information every time we log on to social media or use search engines. But, at the same time, we might hesitate before downloading a government-funded COVID-19 app that will potentially save our lives for fear about how our data might be used.

“We need more debate around the facts,” said Marco Huwiler, Country Managing Director Switzerland, Accenture. “We need more marketing around the facts. Why are people going to social apps but not using the COVID app? Is it related to the personal benefit they see in doing so? Studies show that if people see a personal benefit, they are happy to share data.”

Indeed, when we interface with an information exchange or sign up to social media online, we engage in a “privacy calculus”, weighing up the various pros and cons for each specific context. Users can also suffer from a “privacy-personalization paradox” – where we want to receive services that are tailored to our own needs, but we do not want to give away too much information to get that desired level of personalization.

The challenges facing individuals range from these dilemmas to the implications of outright overuse and misuse, bias, privacy abuses and malpractice.

Educate to empower

The current status quo, where individuals do not know enough about what is happening to their data or how to manage their information online and also do not receive a cut of any financial gain from data use, needs to change if society wants to reverse the erosion of trust in digital technologies.

This probably starts with education – of the risks, the technology and the tools to manage it properly on an individual level.

“Only informed, educated and tech-savvy citizens will feel at ease and empowered to use new technology and tools,” said Niniane Paeffgen, Managing Director of Swiss Digital Initiative, which seeks to safeguard ethical standards in the digital world.

“Lifelong learning is key to make sure the digital divide does not deepen further but can begin to heal,” she said.

82% of the Leaders of Tomorrow consider easy access to information about how one’s data is used as an urgent or at least necessary means to increase trust in technology.

75% of the Leaders of Tomorrow agree: "My generation does not do enough to combat the effects of fake facts amplified by new technologies." [2]

SDI also drives the development of an independently verified digital trust label, which would set and require certain standards on digital ethics, data, reliability and security, giving consumers a reason to trust providers and companies.

Beyond education, there is a need to increase the power of individuals to manage their data online and how it is used, for example, with a right to review usage.

A right to review and share in the rewards?

"The notion of approximate data privacy encroachment is now a reality," said Jeffrey Bohn, Senior Advisor at the Swiss Re Institute. "Anyone with basic modeling capabilities and an internet connection can find out approximately – to a level of statistical confidence – many things about you as an individual without ever directly breaching a privacy-protected database."

"In addition to the right to delete, which is part of GDPR, we should have the right to review," he argued, suggesting that this would enable individuals to ensure that any data kept online about them is accurate and up to date. It would also address the unintended consequences that are created when data users share online is then combined with other publicly available datasets.

With more and more companies making money from data, Benedikt Schuppli, the Co-Founder and Co-CEO of Swiss fintech FQX, is among the voices calling for a way to allow users to share in the financial value of data harvesting.

"Data protection should be replaced with the concept of self-sovereign identity - the self-sovereignty of every data subject regarding the data that relates to them and that can be monetized by them because currently they are not receiving anything of that," he said.

Big tech firms argue that tools have already been introduced to help individuals control the use of their data online, but few users are aware of these powers or how to use them. Platforms, for example, allow users to see what data is collected and to delete or export it.

"When we talk about privacy and data, it is also very important to think about security and encryption and how we educate and help users so they know about these options so they can use them," said a senior executive at a global tech firm. "I believe we can still improve. We try to help them know about these options, but not all social media platforms help their users know about their options."

Tech can help address the tech trust crisis

Digital solutions for digital trust already exist, but there also needs to be a forward-looking, integrated approach to innovation that factors in ethics, security and privacy from the start.

While companies, governments and individuals search for answers in managing data, privacy and security, the solutions to large parts of the crisis of trust in technology already exist in the vast realm of digital innovation itself.

The hunger for data analytics and the misuse of that information may have eroded trust, but technologies such as confidential compute and advanced encryption can help to restore faith in the system – if they are properly implemented.

"There are important cryptographic primitives, such as homomorphic encryption, or other secure multi-party computation methods that exist already and can be used in many cases in order to achieve higher privacy guarantees," said Katerina Mitrokotsa, Professor of Cybersecurity at the University of St. Gallen. "Many companies are not aware of these technologies and they have not adopted them."

One concept that offers hope is self-sovereign identity. This is achieved through similar technology that makes blockchain an increasingly popular way to manage online transactions and interactions where trust is key.

"Maybe this is more about education and regulation, really explaining to people how they do self-sovereign control of their personal data, in particular, vis-à-vis distributed ledgers," said Swiss Re Institute's Jeffrey Bohn, referring to the technology which creates transparency by sharing information between parties in a decentralized way.

These technologies can help to establish trust between parties in the online world, where it can be difficult to verify the identity or credentials of others.

Data analysis without eroding trust

At the same time, in response to user fears that companies and governments might be using personal data way beyond any agreed or expected remit, the adoption of confidential compute or homomorphic encryption offers a glimmer of hope.

These technologies create a bubble around personal data through encryption or protected enclaves, while also allowing third-party entities to access it without compromising privacy or security.

However, while these tools exist, they are only part of the solution to a deeper problem at the heart of digital innovation.

7% of the Leaders of Tomorrow would rather rely on AI than on a human psychotherapist.

63% of the Leaders of Tomorrow say it is essential to have transparent privacy measures for safeguarding customer data in ecommerce. [2]

As IMD's Professor Öykü Işık pointed out in the spotlight feature at the start of this report, biases and long-term risks can creep in at the development stage of new technologies because they are created by imperfect humans.

Unless an enlightened approach to ethics, privacy and security is integrated right at the beginning of the creation of digital products and services, we will continue to build a suboptimal digital world prone to crises of trust.

"We have to deploy and fix the security by design from the very beginning," said Professor Mitrokotsa. "We need to rethink the tools – having more decentralized tools and not this centralized model gives better transparency but also a better way to avoid single points of failure when we have data breaches.

TECH'S TRUST SOLUTIONS

Self-sovereign identity (SSI) features credentials that have been verified by trusted issuers and can be used by various parties during an interaction or transaction. Users control these credentials, the related identifying components and their use, creating a decentralized system of trust.

Confidential compute enables sensitive data to be protected and isolated so that it can be processed securely in the cloud. This can be used for financial information or for personal health records. It allows for function such as analytics and machine learning to take place without compromising personal privacy or security.

Distributed ledgers create a decentralized peer-to-peer network which allows for each entity to access, update and hold the ledger independently. The ledger is led by consensus, without a central authority, meaning that any update must be approved by all parties.

Homomorphic encryption permits users to process encrypted data without having to decrypt it first. This means raw data can be analyzed by third parties for, say, commercial or scientific purposes without revealing any identities or compromising security.

Cryptographic primitives are the algorithmic building blocks of security protocols and systems such as encryption.

Showing leadership and taking responsibility

Not enough companies are embracing the digital tools available to safeguard trust and lean too heavily on imperfect self-regulation. A code of conduct could help reduce incidents of corporate malpractice and data abuse.

While it is tempting to think that the only solution to corporate overreach when it comes to data is tougher legislation, one of the biggest hurdles to restoring trust is that companies are slow to integrate and make the most out of technological solutions that already exist.

"Regulation is an important part of the solution, though not the only one. There is a lot that companies themselves can do to adopt practices and policies voluntarily," according to Manju George, Head of Strategy, Platform on Digital Economy and New Value Creation at the World Economic Forum.

"There are technological and legal and other innovations that can unlock valuable insights from data while protecting the interests of different stakeholders. Yet, they are still not adopted widely. You don't have to wait for regulation," she said.

Self-regulation must be robust

In addition to the using digital innovation to strengthen trust, it is important that companies and organizations step up when it comes to designing more robust internal policies and practices as part of necessary self-regulation in a fragmented (in terms of legislation) global marketplace.

"We will need regulation and we need standards, but we really believe in the meantime in organizational accountability and shared responsibility," said Sophie Batas, Director for Cyber Security and Data Privacy at Chinese tech firm Huawei.

For this approach to be robust, however, companies must be consistent and credible in their approach to self-regulation and in the protection and guarantees they provide customers.

"Politics needs to set frameworks and conditions to make sure trust can grow, but business must also live up to its societal responsibility," said Swiss Digital Initiative's Niniane Paeffgen.

It also means more joined-up thinking when it comes to customer needs.

"We need cloud providers like Google or Telekom or Microsoft in Europe that really can ensure, from a legal standpoint, that they actually process the data only within the European Union," said Jonas Muff, CEO and Founder of Vara, which has developed AI software to improve the screening of breast cancer through the analysis of patient data.

78% of the Leaders of Tomorrow agree with the statement "Most online companies and platform providers do not do enough to flag and prevent fake reviews." [2]

Holding malpractice to account

In a world of data breaches, exploitation and overreach, it is clear that many companies have a way to go before regaining public trust in the digital space.

Some experts suggest the establishment of a tech industry code of conduct that could mirror practices in the medical profession would give more credibility to self-regulation.

Marianne Janik, Area Vice President for Microsoft Germany, cited the idea of a "Hippocratic oath" for the tech world – where concepts such as "first, do no harm" could create a sense of human purpose and greater responsibility in the industry. This oath concept, which has been in the ether for several years, would also help to reassure users that their needs are being considered at development stage.

"Privacy is a human right," she said. "People will not use technology if they do not trust it."

Others, such as Bohn, think tougher and bolder industry measures may be needed, including an enforceable framework for malpractice based on certification under a code of conduct.

"We need to develop a sense of what constitutes malpractice in algorithmic development and machine intelligence deployment," he said. "We talk a lot about bias and ethics, but if we don't have mechanisms to go after the vulnerabilities, it will be difficult to improve over time."

Towards a future of digital trust

Many of the questions at heart of the digital trust crisis can only be answered at societal level. More opportunities for dialogue between all stakeholders are required alongside more support for public-private partnerships, and the harmonization and proper implementation of more agile legislation.

With so many conflicting interests and voices in the digital space, agreeing a shared way forward is proving a challenge. However, the looming crisis in trust has focused minds around the ethical dilemmas and regulatory responses that must now be shaped at societal level.

"Trust in ICTs is vital for not only achieving the (UN) Sustainable Development Goals, but also to accomplish the societal-level digital transformation that we are going through," said IMD's Professor Öykü Işık.

It is clear that the solutions for the complex and far-reaching ethical and economic challenges lie beyond the reach of industrial self-regulation, individual action or technology. Indeed, the focus of legislation may have to shift to further protect the interests of individuals and society.

"Data governance should protect the powerless. We should move from data protection to data emancipation," FQX's Benedikt Schuppli argued.

Digital outpacing policy

The problem so far has been that the traditional snail pace of legislation cannot keep up with technological change, creating tension between private sector innovation and public sector governance.

"The speed of technological development is growing exponentially and law-making will not be able not to adjust to this pace if it tries to regulate each and every detail. It needs to happen on the right meta-level," observed Accenture's Marco Huwiler.

"As soon as we see a good collaboration between public and private sectors, things can be solved effectively. The moment we have this bipolar world of public against private sector and we are looking to the public sector to solve these topics alone, it will not work. It takes at least two to tango."

Indeed, experts at the St. Gallen Symposium repeatedly called for more opportunities for dialogue and exchange between private and public sector actors, as well as the creation of more opportunity for public-private partnerships, with both sides eager to find the right solutions that can rebuild trust while supporting innovation and economic progress.

"On the one hand, you have public governance needing to protect citizens' rights and to protect against the misuse of data. At the same time, there is a need to create the space for private sector innovation as well. There is this perception ... maybe a reality, of public sector governance trying to play catch-up with private sector innovation," said Kulani Abendroth-Dias, Strategic Analyst at OECD.

"How can we better manage and enhance this relationship and understanding between public sector governance and private sector innovation, so that countries and regions don't fall behind? How can we contribute to smart, effective regulation together?"

Part of the solution means national and regional policymakers working with the private sector to create clear, agile regulations that are fit for purpose in a rapidly changing environment and hardwired to promote trust.

"The best practice would be to follow a data minimalist approach to make sure we collect as little data as possible, while at the same time, providing good guarantees and good services depending on what we want to achieve," said Professor Mitrokotsa.

The WEF's Manju George cited work on technology governance that her organization has been engaged in

66% of the Leaders of Tomorrow think their generation does not put enough emphasis on ethical standards in new tech. [2]

with governments, the private sector and other stakeholders to inform better policymaking for topics such as AI, data and blockchain.

"More spaces like that, which connect governments, business and civil society would be helpful," she said.

In search of harmony

But enhancing the policymaking process will only have real impact in building trust for users and companies if it is collaborative, consistent and harmonized across borders to iron out imbalances and loopholes in the system.

"There is a need first to align in Europe because the fragmentation is very high, but the next step is to align globally and the two processes should be done in parallel," said Huawei's Sophie Batas.

"It is really a right moment to create a digital forum for all these issues that will involve the right people in a coordinated process," she said.

An indication of the complexity of this task can be seen in the way that GDPR has been managed in the European Union.

"GDPR was a great step forward for the European Union, but the problem for us is at a practical level every country in Europe implements GDPR differently, which creates legal uncertainty and makes it very difficult for young companies like mine with limited resources to navigate," said Vara's Jonas Muff.

Beyond legislation and greater collaboration to tackle cyber security threats and data breaches or misuse, there are potential lessons to learn from the way society has tackled other industrial challenges.

For example, the creation of an independent authority that could investigate data breaches or cyber attacks and publish its findings could help to reduce the risks of future digital crises and shore up trust.

"We should have the equivalent of the US's National Transportation Safety Board (NTSB – focuses on finding out causes of large transportation accidents) for looking at IT system failure or large cyber hacks, so you have a mix of technology people, lawyers and regulators that can go onsite and figure out what went wrong and publish the technical details, so it doesn't happen again," Bohn said.

While oversight of data protection law is covered by data protection authorities in Europe, there are limited opportunities for lessons to be shared and learned across industries so that history does not repeat itself. Some companies engage investigators when breaches occur, but these findings tend to be kept internal for confidentiality or competition reasons.

As an alternative to investigations, and given the need for greater collaboration to solve digital's trust crisis, less formal platforms for information sharing and consensus building should also be supported.

The Cyber Security Coalition in Belgium, for example, acts as a platform for information exchange between stakeholders to build resilience. In addition, if there was a global consensus, for example, not to pay when criminals unleash ransomware attacks, this model would be become less viable over time.

CONCLUSION

Securing the four building blocks of digital trust

By focusing efforts on the building blocks of individuals, technology, organizations and society, all stakeholders can work together to regain and safeguard trust in the digital world in order to realize the great promise of technology.

While the challenges are great, the solutions for fixing the looming digital crisis of trust lie within reach.

However, experts agreed that these solutions will only be found through an enhanced effort by all stakeholders to take responsibility and work together with a shared vision of trust.

Within this, each of the four building blocks outlined in this report must be addressed as part of a comprehensive and holistic approach to building a digital world that is safe, secure and fair.

From harmonizing legislation and embracing more robust self-regulation to taking advantage of digital tools that already exist and granting greater powers and rights to users, the expert insights offered in this report can contribute in a meaningful way to building that world.

Without concerted action across each of the four building blocks, the digital space is likely to continue to suffer from an erosion of trust in ethics, privacy and security, which will have lasting repercussions for our shared economic and societal destinies.

ACKNOWLEDGEMENTS

Öykü Işık, Professor of Digital Strategy and Cybersecurity at IMD, Matt Falloon, IMD Editor, and Felix Rüdiger, Head Content and Research of the St. Gallen Symposium are the co-authors of this white paper. They would like to thank the participants of the roundtable “Strengthening Trust in Technology When It Matters Most” on 5 May on the occasion of the 50th St. Gallen Symposium for sharing their valuable experiences and insights.

To cite the white paper, please use: IMD and St. Gallen Symposium (2021) Strengthening Trust in Technology When It Matters The Most. Joint White Paper.

REFERENCES

1 Vinuesa, R., Azizpour, H., Leite, I. et al. The role of artificial intelligence in achieving the Sustainable Development Goals. Nature Communications 11, 233. 2020. https://doi.org/10.1038/s41467-019-14108-y

2 Gaspar, C., Dieckmann, A., Neus, A., Kittinger-Rosanelli, C.: Voices of the Leaders of Tomorrow: Challenges for human trust in a connected and technology-driven world. Nuremberg Institute for Market Decisions and St. Gallen Symposium. 2021. https://www.symposium.org/sites/default/files/2021-05/VoLot%20Report%202021.pdf

The “Leaders of Tomorrow” are a carefully selected, global community of the most promising young talent. Each year, 200 academics, politicians, entrepreneurs and professionals aged around 30 years or younger represent the voices of the next generation at the St. Gallen Symposium. Leaders of Tomorrow qualify either through our global essay competition aimed at graduate students, or they attend based on their professional or academic merit through a strict selection process. After the symposium, they join the Leaders of Tomorrow Alumni Community, which has over 2,000 members worldwide.

IMD

REAL LEARNING. REAL IMPACT

ST.GALLEN SYMPOSIUM