Accountability Paper
→ Vision 2020

Taking Stock & Looking Forward

INSTITUTE FOR
ACCOUNTABILITY
IN THE DIGITAL AGE

www.I4ADA.org

In Memoriam

† January 2019
This Vision Paper is dedicated in memory of the late Dr. Indrajit — Jishu — Banerjee, Director Knowledge Societies UNESCO. Dr. Banarjee was the spark for our global and multi-stakeholders' discussions on Accountability in the Digital Age.

Contents

Click on the text to go to the chapter

Preface

5 Questions about this Accountability Vision Paper 2020

1. Why this Vision Paper?
This Vision Paper is by made by Institute for Accountability in the Digital Age (I4ADA) and is aimed to provide some relevant oversight and insights on the state of play and state of the art of Accountability in the Digital Age.

It is doing so by both taking stock of the take-aways from the The Hague Summit 2019 organised by I4ADA, from other relevant developments, as well as by using these for forward-looking considerations, future activities and other further developments.

This Vision Paper does not have the ambition to be complete or exhaustive.

2. For whom is this Vision Paper?
This Vision Paper is meant for both the public sector and private sector, either large or small and in any part of the world, as well for NGOs, academia, organisations and last but not least individuals that are interested in these vital topics and discussions.

3. What is I4ADA?

I4ADA is the abbreviation of the Institute for Accountability in the Digital Age, a not-for-profit foundation under the laws of the Netherlands, based in The Hague.

4. Why Summit 2019?
The Hague Summit 2019 was a two-day conference in the Peace Palace in The Hague, The Netherlands. It brought together a global multi-stakeholder community from national and local governments, international policy makers, civil society, NGOs, the IT industry and platforms, as well as other relevant organizations, institutions and individuals, the latter with an age ranging from 17 through 83 years old.

The main aim was that the delegates' recommendations further contributes to shaping a global path towards each stakeholder in this Digital Age acknowledging and investing in their individual as well as collective respective level(s) of continuous appropriate dynamic accountability.

The main focus for The Hague Summit 2019 was on the how; how to get to those appropriate levels of accountability in this Digital Age, who are the stakeholders in each of the relevant domains and dimensions, what does it take, and which instruments are necessary, to be developed or already available.

5. What's next?

The Institute will use the oversight and insights in this Vision Paper for its next activities, including explorations, discussions and development of 21st Century instruments for Accountability in the Digital Age, as well as the preparation and feeding of its next events, either virtual, physical or hybrid.

Please check our website periodically. Furthermore, please follow the Institute via social media including LinkedIn.

Recap Summit 2019

i4ada.org/recap-summit-2019

The 2019 Summit was fully recorded.
Please click on the links to watch back the recordings.

Video registration recorded by

SDGHUBNL global goals, local impact

Summit day 1

November 6th 2019 – Keynotes and paneldiscussions recorded at the Peace Palace, The Hague, during the I4ADA 2019 Summit

Click here to watch the videos

Summit day 2

November 7th 2019 – Keynotes and paneldiscussions recorded at the Peace Palace, The Hague, during the I4ADA 2019 Summit

Click here to watch the videos

Download the presentations

A selection of panelists provided us their presentations for availability online. You can view / download the individual presentations at your convenience

Click **here** to view the presentations

Summit 2019 images

Have a look at the photos of The Hague Summit for an Accountable & Democratic Internet: The Internet of Values

Click **here** to view the images

Introduction

Accountability Vision 2020

In this Vision Paper we will explore multiple domains and dimensions related to Accountability in the Digital Age. With this, we aim to provide some relevant oversight and insights on the state of play and state of the art of Accountability in the Digital Age.

We are doing so by both taking stock of the take-aways from past events such as the The Hague Summit 2019 organised by Institute for Accountability in the Digital Age (I4ADA), as well as from other relevant developments. Additionally, this Vision Paper takes these in for forward-looking considerations.

I4ADA hopes this Vision Paper is beneficial both for you as reader as well as for further discussions and developments you may be part of.

Institute For Accountability In The Digital Age

Technology changes the world at a fast pace. On 6 August 1991 the internet became publicly available through the World Wide Web. A new technology which would fundamentally change the world as we then knew it. Today we see more than 50% of the world's population; a number that increases every day.

Societies and individuals can benefit in all manner of ways through access to knowledge, people and organizations on a local and global level. More than that, digital has become a must-have, for people, society and the economy. Indeed, digital technology fosters innovation. Online platforms, e commerce, social media, artificial intelligence, data analytics, robotics and the internet of things (IoT) are further expediting this process by hyper-connecting individuals, organizations, communities, societies and data, with tens of billions of objects and entities.

Unfortunately, the Internet is not immune to evil. Breaches of norms and values are also occurring in the online and cyber world, ranging from fraud, identity theft, bullying and other forms of personal harassment or exploitation through to malign social engineering, phishing and hacking attacks which can threaten key networks and even entire nations. Fairness, transparency and accountability dictate that any victim, — whether individual, organization, society, nation or even democracy itself — which suffers from these issues should be able to address those responsible and to secure meaningful, effective redress. However, we are in a position today, in this Digital Age, where ongoing technological developments have outstripped our policy-making capacity, standards-setting and legal frameworks.

The Institute was founded with the mission to ensure that those issues and concerns do not undermine the Internet's potential for increasing access to knowledge, spreading global tolerance and understanding, and promoting sustainable prosperity.

In pursuit of its mission of helping the world derive maximum benefit from the internet, the Institute is dedicated to helping create a fair and balanced framework of best practice and, where necessary, regulation. Among other activities, these are the main activities of the Institute:

A. Create awareness for Accountability in the Digital Age
B. Host a global multi-stakeholder community
C. Provide knowledge sharing on Accountability in the Digital Age
D. Explore and develop 21st Century instruments for Accountability

The Institute will pursue its objectives by building ongoing dialogue, both structured and informal, among participants in the internet environment. By building and maintaining a network at national and international level bringing together stakeholders and organizing activities, meetings and congresses to highlight, support and facilitate accountability nationally and internationally. These stakeholders represent participants from civil society, academia, the business technology community, lawyers and policymakers.

Chapter
1

The Hague Charter for Accountability in the Digital Age

The Institute has initiated the creation of the 'The Hague Charter for Accountability in the Digital Age'. The objective of these Principles is to provide a guideline for a structured and continuous discussion on Accountability in the Digital Age. It also aims to develop an international community on this topic.

Over the past two years, the charter of the Institute called 'The Hague Charter for Accountability in the Digital Age' has been created in collaboration with UNESCO and The Hague, and further evolved by means of numerous recommendations and other input of various institutions and experts.

The Charter offers a framework of various domains, dimensions and initial main principles for future dialogues and initiatives regarding accountability in the Digital Age. Such include, without limitation, engagement and development of possible instruments on regional, national, international or global level to cater for the uptake and sustainment of accountability in the Digital Age.

The initial first draft Charter as presented and discussed during the Summit 2018. Thereafter, a public consultation of the draft Charter with the delegates of the Summit 2018 was organized. The aim was to assess if these concept Principles would offer value to the global discussion on Accountability in the Digital Age. Various stakeholders provided recommendations and other feedback. Following the Summit 2018 and during the period up to the Summit 2019 the Institute received additional suggestions for improvement. All changes have resulted a major update.

The current version of the Charter is set forth below and is also available online. The Charter is used as the guiding principle for all presentations and discussions, including those of The Hague Summit 2019.

The Hague Charter for Accountability in the Digital Age

The digital world is changing everything. Whether purely digital, cyber-physical or otherwise. And in any context.

As much as the bounties of the Digital Age are improving our lives and economies, it is changing the way individuals and organisations communicate, act and react to each other. Interactions in the Digital Age are complex and raise a number of questions including the protection of human rights, integrity and dignity, and the lack of transparency and accountability.

As Internet has become a need to have, not a nice to have, failure to protect and defend personal and societal rights, integrity, dignity and other values in the Digital Age can have devastating consequences. These human and societal values need to be protected from malicious acts and other threats, and the bounties of the Digital Age distributed.

An internet, where each stakeholder is accountable for the consequences of acts and omissions, accountable to others and to society, is integral and crucial to the success of the digital society and economy.

Accountability may refer to personal, social, professional, economical, ethical, philosophical and legal factors and, in this context, principally refers to the duty for internet actors to demonstrate the appropriate levels of accountability, be responsible for the consequences of their actions and to operate within the confines of the rule of law. It also refers to an open, accessible, secure, resilient and accountable internet for all, in line with universally recognized human rights and fundamental freedoms.

The Hague Charter for Accountability in the Digital Age seek to uphold such human-centric and accountable Internet, encompassing all Internet- and cyber-physical-related applications from artificial intelligence to the internet of things, which are essential to the building of sustainable societies and economies in the Digital Age, and the achievement of the 2030 Sustainable Development Goals Agenda.

Individuals and societies need to be able to trust that their personal integrity, democratic and societal values and rights are safeguarded and protected in the Digital Age. Digitalization and accountability must evolve hand in hand. In order to keep pace with continuous advances and threats, people, communities and organisations in all sectors and communities must join forces and take decisive action.

This requires, where not yet implemented already, making concerted efforts to both protect the integrity and rights of individuals and societies in the Digital Age as well as to protect the integrity of the Internet and related ecosystems, and explore and construct a basis for accountability in a hyper-connected and digital world. One which positions human beings, human rights and universal values at the centre, with the main aim to leave nobody behind.

Our High-Level Key Principles:
With this The Hague Charter for Accountability in the Digital Age, the signing partners outline a meta-framework of key accountability principles that we consider essential, within the existing applicable rule of law, for the protection of personal integrity on and of the global internet, and for establishing accountability and safeguarding democratic values on the Internet for individuals, society and relevant public and private stakeholders. Without prejudice to the existing fundamental rights and related frameworks within the applicable rule of law, we believe that a common goal to be pursued is to strive to position human rights and values at the heart of the Internet and its use.

1. **Internet of Values**: We take these values and perspectives as a starting point for analysis and action:
   a. Human and societal values, including human rights and democracy;
   b. The notion of rights and responsibilities, and finding a reasonable and meaningful balance between them;
   c. The 2030 Sustainable Development Agenda as the overall goal, 169 targets to be achieved and the related indicators, metrics and measures to be contextual yet objective;
   d. Net neutrality as an underlying principle;
   e. Respect for the rule of law;
   f. Multi-stakeholders' participation in a multi-faceted context;
   g. Accessible, transparent, enforceable redress, and measurable remedies.

2. **Accountability** by Default: Adopt the highest appropriate level of accountability and ensure that it is configured into the design of services, ecosystems, platforms, processes, technologies, operations, architectures, and value and business models.

3. **It is Everyone's Task**: Anchor being accountable throughout society including the highest governmental, societal and business levels, and all the way through local, national and international contexts. It is everyone's task to be accountable.

4. **Education**: Include internet accountability and digital skills both in educational curricula as well as career development tools, to facilitate both capacity building and resilience, and to lead the transformation of skills and job profiles needed for the future.

5. **Human-Centricity**: Serve as a trustworthy, guiding and accountable stakeholder towards individuals, communities and society.

6. **Transparent & Technology-Neutral**: Inclusive and overarching principle-based, transparent and technology-neutral approach by default addressing all technologies linked through the internet.

7. **Multi-sectorial Partnerships**: Drive and encourage joint-initiatives and other partnerships between the public sector, private sector and other sectors and stakeholders, in order to implement the principles in the various parts of the digital world without undue delay.

8. **Continuous Co-Creation**: Co-create with a permanent multi-stakeholder dialogue the relevant subsets of principles, parameters, indicators and metrics that may represent the ability of Internet providers and users to be accountable, including but not limited to general awareness-raising, media and information literacy, good practice codes, informed recommendations, statutory legislation or regulation. Apply the expertise developed for the quantification of similar human and societal values to measure accountability in the Digital Age.

9. **Policy Frameworks & Enforcement Collaboration**: Participate in a permanent multi-stakeholder dialogue and network in order to share new insights, information on incidents and trends, and facilitate discussion on effective redress and remedies. Promote local, national, regional and international collaborations in good practices, standardization, regulation and awareness, as well as appropriate, effective and readily accessible alternative dispute resolution and cross-border law enforcement.

Chapter
2

Accountability in the Digital Age: From Why to How

Symbiosis
The real-life world is not only the physical world anymore. The 21st Century real life world is and will be more and more the symbiosis of physical, physical-cyber, cyber and cyber-physical worlds.

Where in the past the physical world was seen leading for people, society and economy, it is clear that the past 20 years have changed that notion. That does not mean that people, society and economy are ready for it, have accepted it or understand it. The transition will take time, will be in multispeed mode, and the symbiosis will vary, include different proportions of these worlds, will be dynamic depending on context and other factors, and will not become static at any point in time.

It is important to note, study and understand human nature in general and per region and culture in particular, as the evolution as humans in the physical world and related very complex societal ecosystems have been ongoing for thousands of years and ' merging' it in the symbiosis as stated above, of physical, physical-cyber, cyber and cyber-physical worlds is a pivotal one.

One of the main reasons why we believe in this symbiosis and that will take place, is that in it reflects the ongoing developments of the past two decades and the expectations of evolution for the next decades to come — where everyone and everything is getting more connected, intertwined and global than before, and start to become more and more interconnected and hyper-connected. –

Therefore, every person, every organisation and every community is relevant and will need to acknowledge the reality, and think about how to organize it for a future-proof, inclusive and resilient future. We need to understand and appreciate how we behave, how we collaborate, what each needs to do to avoid problems and know and communicate beforehand how to resolve problems. Accountability is about owning and co-owning roles and responsibilities, find solutions, make it happen, to help out if things may go wrong once in a while, and to double-loop and otherwise optimize with lessons-learned.

Accountability is not an afterthought dealt with after something goes wrong. It is an essential requirement, both before one acts as well as during and after.

Accountability is also not about blaming others. This also as otherwise one gives up the power of change. And change is the only constant, also in this highly dynamic Digital Age.

The Why
Where nowadays there is consensus on why accountability is important, also when it relates to ecosystems where any form of digital or related technology is part of.

For instance, the Responsibility Principle of the 2015 OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity states:

'All stakeholders should take responsibility for the management of digital security risk. They should act responsibly and be accountable, based on their roles, the context and their ability to act, for the management of digital security risk and for taking into account the potential impact of their decisions on others'.

The accelerating pace of digital transformation combined with the increasing number and sophistication of digital security and threats has created a need to better understand how this principle applies to categories of actors such as product makers, software developers and security researchers. In particular, governments are increasingly interested in new policies that would help enhance the digital security of products, including by encouraging responsible management and disclosure of vulnerabilities.

One of the why's, why the Institute is active as independent and neutral platform regarding Accountability in the Digital Age, is as avoid talking about these topics has led to a lack of understanding.

And understanding — including understanding each other, including each other's various interests and values — is a prerequisite for a future with local, regional and global ecosystems that are transparent and trustworthy and where all stakeholders are co-accountable, for people, planet, prosperity, peace and partnership.

The How
How can we help? The Institute has the objective to promote the accountability in this era of increased technological developments, products, services and complex processes as well as organizational structures. One of the related objectives of the Institute therefor is to help and otherwise contribute to the development contextual instruments and guidance for practical and other policies that will increase transparency, reduce unpleasant surprises in the Digital Age, and most of all increase trust and trustworthiness. Making it work, including the appropriate functionals, non-functionals and related accountability, is complex but that is where the true huge potential is, for all, and the future of mankind and our planet.

How can we all help? During the two-day conference, the 'How' was discussed both from generic and specific perspectives. Both top-down as well as bottom-up initiatives, challenges, best practices and practical use cases and other examples were presented and discussed. Furthermore, the 'How' was discussed in three (3) domains, being on 7 November 2019 (social) media and journalism, and on 8 November 2019 artificial intelligence respectively cybersecurity.

The Hague Summit for Accountability in the Digital Age: From Why to How

On 7 and 8 November 2019, the second 'The Hague Summit for Accountability in the Digital Age' was held, organized by the Institute for Accountability in the Digital Age.

The inaugural 'The Hague Summit for Accountable & Democratic Internet, The Internet of Values' in May 2018 at the Peace Palace in The Hague. It was supported by the City of The Hague, the Dutch Government and UN agencies UNESCO and ITU.

Being the inaugural summit, the main focus of The Hague Summit 2018 was the Why: why is accountability in the Digital Age a topic and dimension to discuss, who are the main stakeholders, and what and where are the main challenges and opportunities.

To further support the development of detailed discussions about accountability, principles and instruments, build momentum, and foster further collaborations at global level, all with the aim of promoting Accountability in the Digital Age, the Institute organized its second summit, The Hague Summit 2019.

As the Institute is designed to be neutral, not for profit, independent and driving and encouraging joint-initiatives and other partnerships between the public sector, private sector and other sectors and stakeholders on a global level, also regarding The Hague Summit 2019 the Institute aimed at an all-angled multi-stakeholders' attendance from around the world, which is has again succeeded in.

As the main focus for The Hague Summit 2018 was on the Why, the main focus for The Hague Summit 2019 was on the How: how to get to those levels of accountability in this Digital Age, who are the stakeholders in each of the relevant domains, what are the various interests and common values, what does it take, and which instruments are necessary, to be developed or already available.

During the two-day conference, the 'How' was discussed both from generic and specific perspectives. Both top-down as well as bottom-up initiatives, challenges, best practices and practical use cases and other examples were presented and discussed. Furthermore, the 'How' was discussed in three (3) domains, being on 7 November 2019 (social) media and journalism, and on 8 November 2019 artificial intelligence respectively cybersecurity.

During the second edition of the Summit in November 2019, various perspectives, key notes, presentations, reports and recommendations were given, discussed and debated. All discussions and documentation presented at the Hague Summit are public.

This Vision Paper does not have the ambition to be complete or exhaustive. All presentations, video recordings and transcribed content of the Hague Summit 2019 sessions can be found at www.i4ada.org.

However, the insights and outcomes from the Summit will contribute to shaping the global path towards ethical and effective cyber policy and development of relevant tools. These developments will enhance the global mission of raising the bar for accountability, and therefore trust and trustworthiness in this Digital Age.

Chapter
3

Accountability & Current State of Play

Introduction

↑ Saskia Bruines welcomes everybody on behalf of the City of The Hague

The current state of play of accountability in the field of technology and societal challenges and opportunities shows all different levels of maturity. The maturity on 'why' is generally sufficient, where the maturity on 'how' is not. The bridge between 'why' and 'how' is where one moves from talk to walk the talk. In this dynamic Digital Age, it has been proven that it is not easy. In most cases the level of practical and operational maturity is quite low, but there are plenty good examples with good practices to take in and other lessons to be learnt from them.

Some current key questions that can be raised are: how does the daily use of technology impact society; who are connected in the digitally fragmented global society and who are left behind; what does the term accountability mean in the Digital Age, and why does having adequate levels of continuous appropriate dynamic accountability in place seems to be difficult?

The Hague Summit 2019 Panel Flow

In the related panel at the The Hague Summit 2019, it was evident to the panellists[1], that technologies have given rise to many opportunities for the humankind, in terms of the free flow of information and knowledge and efficient means of communication. However, in today's hyper connected Digital Age, societies have not always foreseen the dangers of technology, or the socio-cultural shifts that have followed from it. Several panellists agreed that these technologies have significantly altered the way in which we behave and interact with each other in and out of the new digital environment.

As Arthur van der Wees mentioned in the introduction to the panel discussion, accountability has to function both as a 'carrot' to encourage positive action and when necessary as a 'stick' to ensure technology and its use follows our existing Rule of Law, values and ethics through enforceable recourse and remedies.

Sivaaji De Zoysa from the Young Presidents Organization mentioned the deterioration of social norms. Nanjira Sambuli from the World Wide Web Foundation reminded the audience, that the growth rate of people getting access to internet is slowing down

1 The panellists included: Mr. Sivaaji de Zoysa, Managing Director Gaia Investments ltd, Global Chair of the YPO Impact Networks Council, Ms. Kathalijne Buitenweg, Chair of the Committee on the Digital Future, Member of the Dutch Parliament, Deputy leader of the Dutch Green Party, Mr. Nanjira Sambuli, Senior Policy Manager World Wide Web Foundation, Ms. Helen Brown, Legal Council Permanent Court of Arbitration, Prof Mike Hinchey, President International Federation for Information Processing, Mr. John Higgens, Chairman Global Digital Foundation, and Mr. Vadim Belyakov, Founder Not Alone. The moderator was Mr. A.P. Van der Wees LLM, Co-Founder & Board Member I4ADA.

instead of accelerating, thus leaving many people behind from the Digital Age, in particular women and rural communities. Mike Hinchey reflected on the astonishing incivility and hate speech among certain internet users. Vadim Belyakov emotionally and powerfully demonstrated the impact of excessive use of mobile technology on the mental health of young people.

↑ Panel AI — see footnote 1

The panellists agreed that new ethical guidelines and enforceable legal instruments are desperately needed in the Digital Age, and that they will have to be developed at faster pace than ever before in order to sufficiently keep up with the continuous technological innovations and as well as the perceived deviances from our common norms related to human rights, data protection and privacy, and cybersecurity. The harmonized development of these hard laws and commonly accepted soft rules are required to maintain trust and product security in the Digital Age and in order to ensure that technology will have a positive impact on the evolution of society.

Some Other Notable Statements

Throughout the panel it became clear that while technology has been powerful agent for prosperity and innovation, the consequences of extensive use of ICT technology has also generated unexpected divisions, grievances, as well a new types of winners and losers. However, the Internet that we have to come to heavily rely upon is not as universal as we sometimes like to think. Individuals, organizations, and societies have differentiated opportunities for connecting themselves to Digital World.

Nanjira Sambuli noted that the growth rate of people getting access to internet is slowing down instead of accelerating. At the current rate, the Sustainable Development Goal 9C focused on providing universal and affordable access to Internet by 2020, will be missed by about 23 years in the least developed countries. Thus, leaving many people behind from the Digital Age, in particular women and rural communities. This digital gap will drastically influence the types of values and norm that's will be incorporated to and represented in the cyber world.

As new ethical guidelines and enforceable legal instruments are desperately needed in the Digital Age, these instruments must be produced within a multi-stakeholder, multi-disciplinary, and a transparent way to yield the hoped results and in order to benefit all societies and not only those developing the technology. The need for an accountability

enhancing regulatory framework is evident, but it has to be one that ensures that the outcomes are compatible with commonly shared societal values and norms.
The panellists also discussed how a better understanding and a shared definition of accountability can help to address the negative impacts of certain technologies on consumers and users.

'Technology started off with the aspiration to erase the obstacles of space and geography from bringing people together. Unfortunately, we have come to realize the great paradox of the connected world we created. Technology has driven people apart instead of together. It has divided societies like never before and it has promoted individualism over community — one of the biggest issues of the 21st Century.'
— **Sivaaji de Zoysa**

'The mass media and the popular press have completely conflated the idea of AI and automation. They are not the same thing. Automation may take some techniques from AI research such as voice or facial recognition and lots of other amazing stuff that are great individual bits, but just because you use one thing that comes out of AI research does not mean that you are building an AI system and certainly does not mean that you are applying it.'
— **Mike Hinchey**

'We have reached a moment where people have realized that technologies are not developed in neutral contexts. Good intentions may be there, but there has to be certain explainability about how they were intended to work versus how much they match that in reality. It is also becoming clear that those who design, deploy and even invest in technologies, have nuances, biases and worldviews that are backed into them.'
— **Nanjira Sambuli**

'We don't generate random things in computing. It's based on an algorithm somewhere done by a human, so this means, as we heard this morning about judges using algorithms to decide if people should get parole or what sentences they should get. This is actually becoming quite prevalent in certain jurisdictions in the U.S and this is madness. Absolute, madness because the data that's been put in there is random the data, has been biased the data, has been picked by humans from random places. It is far from complete. It's not fair. This brings in issues of ethics and safety, and the legal aspects related to decisions that we might make.'
— **Mike Hinchey**

The currency of trust creates value for humanity in the Digital Age. Society's progress is built on trust and progress falters when trust is called into question, as we saw in the 2008 financial crisis. We learn to trust in a variety of ways, including by the results of our dealings with people and by listening to the opinions of others, and we give more weight to the views of those we come to trust. When people gather in organizations, we learn to trust those organizations in the same way — companies work very hard to become trusted brands. It's difficult to persuade people to do business with you unless they trust you.

Accountability underpins trust. Things go wrong in every aspects of life; we all make mistakes. How we deal with those mistakes makes a big difference and this is particularly true when you are operating in the online world. There are countless examples of how to handle it badly; we all know of cover-ups, obfuscation, denials. In the Digital Age customers are often one step removed and will only keep trusting, and using/buying, if they see transparency and above all accountability. This means both giving an account, (how did the mistake happen?), and taking responsibility — for resolution and redress.

Being in a position to give an account requires an organization to develop a culture of accountability and put in place the right processes and procedures, capturing enough data about transactions, for example, so that when mistakes occur it's possible to go back and understand what happened, how and even why. A culture of accountability helps individuals and organizations learn quickly from mistakes.

The most common form of Artificial Intelligence in widespread use today, machine learning, can make the first part of this accountability — giving an account — more difficult. Explainability is one of the key challenges for producers and users of machine learning. 'I' ve heard machine learning developers say [about a specific algorithm] with some surprise 'we didn' t expect it to do that!'' — John Higgins

It's vital that the writers of these algorithms are given the tools and then use them to anticipate and explain how the algorithm reaches its conclusions in clear and simple terms. Without this the transparency/accountability/trust relationship risks breaking down with serious consequences and even loss of legitimacy. This is true for commercial activity but also in the healthcare, criminal justice, and education sectors too.

Machine learning is perhaps simply the latest challenge an accountable organization must deal with. But organizations which understand that accountability underpins trust will master this challenge. These are the companies, enterprises and public bodies that will prosper and thrive in the Digital Age.

Chapter
4

Accountability & Media and Journalism

Introduction

↑ Panel discussion 'Accountability & (Social) Media and Journalism

If everything can be faked, how can we know if anything is real. Media and journalism are prerequisite for society. What to believe and what not to believe?

Some current key questions in this domain are: how can digital technology, journalism and public media improve accountability; what is the difference between traditional media and social media; what are the biggest challenges for upholding accountability in this realm; what is the role of regulation in this realm.

The Hague Summit 2019 Panel Flow

In the related panel at the The Hague Summit 2019, the panellists[2] shared their valuable insights on Accountability in the realm of social media, traditional media and journalism. While digital technologies have served to improve accountability in the news and broadcasting world, for instance by identifying information with questionable sources, they have also offered means to evade accountability and to distort the truth for personal gain. Examples of these incidents are abundant, and they vary from false accounts and identities to misleading political and economic storytelling to outright misinformation campaigns.

Panellists agreed that more clarification is needed on attributing responsibility online, so that now, and in the future, actors can be held accountable with regards to legal rules. In addition, new policies need to be developed to ensure that the technologies we use and build for the cyber sphere are aligned with old and new societal norms and values such as the 'right to privacy', 'freedom of speech' or the 'right to be forgotten'.

This panel kicked off with Vincent Everts, who noted the important difference between content generated by a real person and a bot. Joelle Casteix explained the urgency for making online places safe for all users, including minors. Andrew Taussig discussed the importance of upholding journalists' code of ethics so that misleading or simply untrue stories are not able to skew politics. Nad'a Kovalcikova reflected upon political advertisement on social media platforms and which types of advertisement is more democratic; microtargeting campaigns or political ads.

2 The panellists included Mr. Andrew Taussig, former Director BBC, Ms. Nad'a Kovalcikova, Program manager and fellow German Marshall Fund of the U.S, Mr. Cyril Pereira, AsiaSentinel, Mr. Oleg Volkosh, President Mediaplus Group, Chair YPO Europe, Mr. Charles Groenhuijsen, Dutch Journalist, Mr. Joelle Casteix, Director Zero Abuse Project, Mr. Vincent Everts, Trendwatcher, and Ms. Urška Umek, Council of Europe, and Committee of Experts on Quality Journalism in the Digital Age. The moderator was Mr. Freek Teunissen, NICJ.

Charles Groenhuijsen drove in the point that the best way to fight misinformation is to have an informed audience, something he sees the traditional media has failed to accomplish. Cyril Pereira argued that the objective of journalism has changed from seeking truth to seeking attention. Urška Umek of the Council of Europe spoke from the perspective of a European policy maker on how online accountability can be upheld through standard setting and co-regulation. Oleg Volkosh shared touching remarks concerning the impact of social media on the mental health of young people, in addition to explaining the technological means we have for large-scale suicide prevention.

Some Other Notable Statements

The key challenges of the Digital Age sometimes have more to do with agreeing on a set of societal norms rather than drafting specific regulation. Similarly, to the offline world, people tend to disagree on the relative importance of certain values. Some people value safety over privacy and some believe in the intrinsic value of anonymity while others emphasize the importance of verified accounts. Therefore, in order to solve many of these challenges related to media, social media and journalism, we need to develop a clear understanding of what values we wish to protect and to what extent we tolerate deviances from them.

Joelle Casteix from Zero Abuse started by pointing out that we need to clarify our social contract as human beings before we can effectively translate our values and rules into the digital space. She stated: 'It is vitally important that as we move with our tools and with the Internet itself, that we understand what is the social contract we have as human beings and to how do we translate that social contract into regulations where we have a safe Internet that allows for full participation but also verified and safe participation for everyone involved.'

Complex questions such as should governments be allowed to tune into private chat rooms for self-harm prevention (i.e. predictive analysis and pre-emptive action). Or would these monitoring services be considered a serious breach of privacy? Data protection and basic human rights need to be solved before moving onwards.

Nad'a Kovalčíková added, 'When we discuss Accountability, we have to also clarify what we are trying to achieve, what are our goals, why are we trying to make companies accountable and based on what principles. Us coming from this democratic, value-based, ethics-based society we have to think beyond progress or what works for everyone. Internet and social media should abide by the values that we cherish. We should not reduce ourselves and our principles to the lowest common denominator when we think of the multi-stakeholder approach.'

When discussing how online accountability can be improved by public media and journalism, the former Director of the BBC, Andrew Taussig, explained the increasing importance for journalists to have a solid code of ethics in their duty to keep the public informed. He shared his definition of journalism, which informed that the responsibilities of a journalist go far beyond simply collecting, writing and reporting news. He states, 'Journalism is professionally gathering, verifying, analysing and presenting facts, especially new facts so as to keep the public freshly and truthfully informed about issues which matter to them and the society'. Journalism is a quest for truth not for clicks or attention.

A similar notion was emphasised by Cyril Pereira who explained the changing nature of journalism, and how increasingly less time and resources are allotted for journalists to conduct thorough analysis and more resources are directed towards capturing people's attention. Attention becomes a product, which is then able to be monetized through advertisements. He states, 'the pressures on online editors is to attract traffic and it is a devil's bargain'. He explained that instead of reader's paying for news, all information is free, which means that the audience becomes the product to be sold for the advertisers, instead of the customers that the newspapers industry caters for. This means that the focus of journalism shifts from quality content to sensational headlines and anything that will rank high in virality.

Charles Groenhuijsen touched upon the abundance of misinformation in online spaces. He shared that the percentage of misinformation is anywhere between 1 to 7 percent of the total stream of information. He argued that the best way to fight fake news and misinformation is to have an informed audience. Highlighting once again, the importance of upholding the mainstream media accountable for effectively informing people instead of provoking fear or capturing monetized attention with sensational headlines. He stated, 'I would like to see more accountability on the part of the mainstream media, because

they determine in ninety-six percent of the cases what's in your newspaper, on your website, on TV.'

The spheres of media, and in particular social media, have become increasingly powerful platforms for influencing and partaking in politics. However, the topics discussed and debated in social media tend not to be proportional to their impact. While large and complex social issues, such as inaccessible housing and healthcare, are often lost in the abyss of information, emotional and explosive opinions by competing political perspectives tend to be highlighted by the algorithms that maximize user engagement. This has created more partisanship and disenfranchisement in both mature and emerging democracies.

Urška Umek reminded us that these social media platforms have an astonishing amount of power to affect global politics. She explained: 'the rise of powerful *private* actors in international law is quite novelty'. The fact that certain social media platforms have more power and money than Member States forces policymakers to interact directly with social media platforms, thus acknowledging their influential role. However, with this power comes great responsibility and policymakers are trying to understand how to navigate this new balance of power. The Facebook hearings of 2019 demonstrate the urgent need to keep the directors of social media platforms accountable for what happens in their forums.

This tied well into Cyril Pereira's point about the partisan-controlled information in the midst of political upheaval. In Hong Kong, where the recent democracy protests have captured the world's attention, and where Pereira currently lives, social media has become an effective tool to promote and recruit for either side of the argument. According to him, the information presented on each side has been highly selective creating echo chambers of partisan knowledge. These secluded echo chambers reinforce favourable facts on both sides and can make constructive discussions between different groups nearly impossible especially when the facts are hand-picked by each side.

Oleg Volkosh exemplified this need to keep social media platforms accountable for what takes place on their platforms with real-life statistics from Russia. According to Volkosh, in one month alone, more than 10,000 suicide notes were left on social media in Russia. The social media platforms have the ability to use the massive amount of data they gather every day for saving lives, polarizing conversations, selling ads or influencing global politics.

Considering how large portions of our lives are spent online, we need to ensure that the spaces in which we connect, seek information and share thoughts and ideas are built, developed and enhanced with our societal values and priorities in mind. This means that we need to start closely observing who is guiding the conversations, who is choosing the agenda, who is benefitting from our attention, and whose facts we are listening to. It is not an easy task, but ensuring that these online spaces are safe, inclusive and transparent is a key component for healthy democracies and human flourishing.

Chapter
5

Accountability & Artificial Intelligence

Introduction

Accountability is not about how one behaves; it is about whether one has made prior considerations and an informed decision how to behave, and whether one can explain (and where necessary: defend) its behaviour.

How does that work in the vast domain that is Artificial Intelligence? What are the accountability needs in developing and utilizing artificial intelligence and explored the many challenges and opportunities that we are facing in light of these emerging and maturing technologies?

↑ AI panel

Some current key questions that can be raised are: what are the key issues and potential solutions when it comes to AI and accountability; how can we regulate AI development effectively; how can we bring everyone at the table for AI discussions; how can we draft legally binding norms without hindering innovation.

The Hague Summit 2019 Panel Flow

In the related panel at the The Hague Summit 2019, the panellists[3] highlighted the various weaknesses in legal and regulatory environment concerning artificial intelligence (AI) and accountability. The evident gaps in regulation on one hand allow companies to leap-frog technology to new spheres with astronomical speed, and on the other hand gives space for those companies to purposely or by accident misuse a technology that is not yet fully understood. How it is possible to find a perfect ratio of accountability-inducing regulation and the necessary freedom to develop advanced versions of AI in a safe and inclusive manner, remained contested by the panel.

Evert Haasdijk displayed the danger of AI technology when it is non-intelligent but extremely efficient. Peter Batt emphasized the need to narrow the distinction between the online and offline world. Cédric Wachholtz highlighted the importance of including all perspectives to this conversation, in particular the Global South. Chrisyina Caljé spoke from the perspective of a company utilizing AI and how they avoid machine learning bias through human assessment (a form of self-regulation). Irakli Beridze raised the question of what are the real, most immediate and practical dangers of AI. Stephen Ibaraki discussed opportunities AI technology brings in solving some of our most pressing global challenges.

3 The panellists included Mr. Peter Batt, Director General German Federal Ministry of the Interior, Building and Community, Mr. Stephen Ibaraki, Managing Partner REDDS Capital Investors, Prof. Tatjana Welzer Družovec, University of Maribor Institute of Informatics, Mr. Irakli Beridze, Director AI and Robotics lab UNICRI, Ms. Christina Caljé, CEO & Co-founder Autheos, Mr. Lukas Roffel, Chief Technology Officer Thales, Prof. dr. Holger Hoos, Head CLAIRE, Mr. Evert Haasdijk, AI Expert Deloitte, Ms. Clementina Barbaro, Committee on Artificial Intelligence of Council of Europe, and; Mr. Cédric Wachholtz, Chief of Section ICT's in Education, Science & Culture, UNESCO. The moderator was Ms. Berenice Boutin, Researcher International Law of Asser Institute.

Lukas Roffel reminded that AI has been around for decades and that it is more present in our society than many fathoms. Holger Hoos defined AI as 'the automation of computer programming'. Clementina Barbaro reminded us that considering that the discussion is already focusing on accountability instead of general ethical principles shows that we have taken steps towards practicality. Tatjana Welzer Družovec brought the focus on the human side of AI development and the need to educate students studying and building AI on the topic of ethics.

Some Other Notable Statements

The panellists agreed that the conversations about AI tend to be general, and what companies and organizations need is practical and enforceable rules and legislation in order to develop AI in a safe, inclusive and transparent way.

Professor Holger Hoos defined AI in the panel as the 'automation of computer programming'. In addition, he clarified that the real concern regarding AI is not 'some sort of strong AI that takes over — that's what we see in movies' but rather the use of already existing AI technology without fully understanding its complexity and 'how things interact right causing inadvertently a lot of damage'. He exemplified this by the Boeing 737 Max tragedy in which the AI technology used was too complex for the staff, regulators or even the pilots to understand leading to the loss of hundreds of lives.

Peter Batt shared his concern over the fact that we are still segregating between the online and offline world. He stated that 'segregation is dangerous because it gives justification to some people to say 'well I am in another world and I do not need rules.' His definition of accountability 'being accountable is being subject to enforcement' further emphasizes the need to have a rule-based approach to controlling AI development. Without formal rules the society cannot hold developers and users of AI accountable when harm is done.

Irakli Beridze agreed on the urgent need for enforceable rules; 'one of the biggest challenges that we are facing is how to translate these discussions, some of which are very academic and some of which are very practical, into real policymaking and into real regulations and frameworks.' Lukas Roffel importantly pointed out that the issue with creating rules for AI stems from the fact that the AI product you develop or sell has the possibility of drastically changing after the of its completion or purchase depending on the date input the user employs– making it more difficult to attribute liability.

Different panellists underlined the numerous efforts in academia, think-tanks and conferences as well as at national levels, that have been put in drafting ethical frameworks for AI. For instance, Peter Batt mentioned that the number of existing frameworks is closer to 130. However, no agreed global, uniform accountability framework exists, to manage the risks related to the use and development of artificial intelligence, leaving space for differentiated approached to AI safety and ethics. The ethical AI principles that were raised among the panellists included understandability, transparency, contestability, predictability, privacy, security, trustworthiness, inclusiveness and accountability.

Clementina Barbaro pointed out that 'the Council of Europe is taking a first step to go beyond ethics and to establish a first legal framework for AI' in close collaboration with private and civil society. This is the first international initiative focusing on creating formal legislation regarding AI. There was clear consensus that ethical frameworks are important, but we need to urgently move toward operationalizing those ethical principles into more formal rules and technical certifications.

A discussion on the topic of inclusivity in AI development was also raised. Cedric Wachholtz explained how AI research is predominantly coming from the Global North, and that we need to become better at including all perspectives in these conversations. He stated 'yesterday I showed a graph of 84 ethical AI frameworks and none of those guidelines came from Africa or South America. It is important to be conscious that we are designing and dealing with something which will transform all parts of the world, but not all parts of the world are at the table'.

Along similar lines, Irakli Beridze noted how the development of AI has the opportunity to create unforeseen wealth for few. The existing wealth inequality will be exacerbated if the digital divide that exists between Global North and South is allowed to grow further. Other important points were made regarding inclusivity and AI, specifically related to education of AI developers and the availability of data.

Tatjana Welzer Družovec explained that awareness and inclusivity of cultural differences need to be taught in universities and schools for people and students hoping to develop this type of technology.

Lukas Roffel also reminded us that the data used for AI development needs to be made available for all players– otherwise limited datasets can lead to dangerous biases and outcomes.

Despite the fears it provokes, AI technology provides also immense opportunity for doing good. Steven Ibaraki discussed the possibility of using AI for solving some of our most pressing issues 'the next 10 years are going to determine somewhat to survivability of our species, perhaps because of things like climate change, but AI could help and mediate some of those problems because of the rapid change of innovation'. This machine learning technology is able to make our current processes far more efficient as illustrated by his example 'JP Morgan used to spend three hundred sixty thousand dollars a year on contracts compliance, they can do this in under a minute using different aspects machine learning — it just illustrates that kind of the capabilities or you're looking at'.

Lukas Roffel, from Thales, continued on this point of efficiency stating 'we are only in the first 3-5 percent of what AI will make possible in the coming years.' If humanity is able to capitalize this efficiency for doing good, the opportunities are immense.

Chapter
6

Accountability & Cybersecurity and Cyber Peace

Introduction

One of the main consequences of this Digital Age is convergence. Communication, IT, data, markets, society, non-military and military converge, to become connected, interconnected or even hyper-connected. One cannot speak anymore of linear supply chains. We are in the era of ecosystems, both upstream, midstream and downstream, and generally we are all part of it. How to make — and maintain — these dynamic ecosystems, including its chipsets, components, hardware devices, communication and computing networks, algorithms, data in transit, metadata and data in rest, as well as related services and systems safe, secure, resilient, up to date, trustworthy, and accountable?

The amount of issues related to cybersecurity and achieving cyber peace is very high. In short, one could summarize it to: how we can create social, cultural, legal and resilient frameworks for accountability in the Digital Age, while maintaining the needed flexibility for advancing merit-based innovation for a sustainable, secure, inclusive and future-proof society, economy and planet?

Some current key questions that can be raised are: what are the trends in cybersecurity realm; how can legal mechanisms of accountability be designed for the cyber space; what are the most alarming risks related to cybersecurity; what are the technical issues and trade-offs we have in designing cyber policies?

↑ Cyber panel

The Hague Summit 2019 Panel Flow
In the related panel at the Hague Summit 2019, considering the enormous risks that ineffective cybersecurity poses for global stability, the panellists[4] expressed an urgency for countries to foster harmonization of national laws within the cybersecurity realm. The global regulatory framework for cybersecurity related issues should be developed in order to ensure that proper action can be taken quickly and seamlessly across nation states and by their national security authorities. In addition, standard-setting through legal means and requirements is essential to ensure that companies maintain a sufficient level of cyber protection throughout their supply chains.

The panel began with Jacques Kruse Brandao outlining trends in the cybersecurity realm and introducing the work of the 'Charter of Trust'. Chris Painter discussed the need to hold state actors accountable for their disruptive cyber behaviour on a global level.

4 The panellists included Mr. Chris Painter, Former Coordinator for Cyber Issues US State Department GCSC, Mr. Arda Gerkens, Senator Dutch Parliament, Judge Chang-ho Chung, International Criminal Court, Mr. Prabhat Agarwal, Acting Head of Unit, Online Platforms & eCommerce European Commission, Mr. Pavan Duggal, Advocate Supreme Court of India, Ms. Catherine Garcia-van Hoogstraten, Lecturer & Researcher The Hague University of Applied Sciences, Mr. Jaroslaw Ponder, Head of Europe Office ITU, and Mr. Paul Timmers, Research fellow Oxford University, Digital Enlightment Forum. The moderator was Mr. Jacques Kruse Brandao, Co-founder Charter of Trust, and Global Head of Advocacy at SGS Digital Trust Services.

Arda Gerkens explained how cyber knowledge exists but is not actively applied in the political decision-making and the apathy that exists towards the subject. Paul Timmers discussed how cybersecurity has transformed the notion of national sovereignty and strategic autonomy. Pavan Duggal outlined various legal approaches nations are taking to ensure cybersecurity. Prabhat Agarwal explained the European Union's approach to cybersecurity. Catherine Garcia-van Hoogstraten introduced public-private cooperation as a solution for improving cybersecurity. Judge Chang-ho Chung encouraged the development of an international convention on cybersecurity that would outline the obligations of the states and rights of the data subjects as well as define rules of cybercrime and warfare. Jaroslaw Ponder concluded the panel by noting the diversity of cybersecurity preparedness that exists in different countries and how important it is to reach those gaps for a safer and more secure global cyber space.

Some Other Notable Statements

The cybersecurity sector in the 21st century is defined by digitalization, shortage of cybersecurity expertise, the utilization of state-of-the-art technology in both conducting and preventing cyber-attacks and the variety of new regulations and agencies addressing the issues related to cyber peace and security.

Enforcing accountability in cyber space is a challenge that requires global cooperation. Initiatives like the 'Charter of Trust', a multi-organizational initiative that both promotes cyber trust and mitigates cybersecurity failures in supply chains, are growing increasingly essential, with rapidly evolving artificial intelligence technologies and the rising prevalence of smart connected objects, or 'Internet of things' (IoT). In addition, the pervasiveness of cybercrime and disruptive cyber behaviour by nation states, demands for more multilateral efforts instead of unilateral action by individual companies and nations.

Chris Painter explained how countries need to move from simply naming and shaming disruptive behaviour to imposing predictable and timely consequences on the responsible actors. However, Prabhat Agarwal also noted that sometimes attributing who is at fault for cyber accidents is impossible, 'in many cases there is a distributed failure that leads to disruptions.'

Fortunately, international law is developing in order to meet the needs for stability, security and accountability in cyber space. The Judge Chang-ho Chung of the ICC explained that there is an absence of one global convention on cybersecurity, one that could

clarify the obligations of the states and rights of data subjects. Some countries and regions have drafted their own legislations, most notably the European Union, which has advocated for advancing cyber accountability through regulations such as the 'European Cybersecurity Act' and the establishment of ENISA, the European Union agency for cybersecurity. Other countries are following suit like Russia, China and Vietnam, but there is still more work to be done in negotiating the rules and norms of cyber space and determining proportional and timely consequences for disruptive cyber behaviour. In addition, concepts like anonymity need to be further analysed in the context of cybersecurity.

Pavan Duggal showcased the different types of legislative means governments around the world have taken to secure safety in cyberspace. These ranged from Australia's anti-encryption law to Russia's balkanization of cyber space.

Prabhat Agarwal dived deeper into the European Union's policy on cybersecurity which consist of three pillars 'resilience, deterrence and defence' and is aligned with the EU's belief in international rules-based order. Importantly, Agarwal also pointed out the important trade-offs that happen when determining the individual responsibilities on cybersecurity within an organization 'the narrower focus you have on accountability the more fragile the whole system becomes while the broader you focus responsibility the less implementable the policies become. Panellists agreed that without stated rules and predictable consequences, cyber space remains a free zone for cyber warfare and cybercrime and accountability, a distant ideal.

Cybersecurity is also transforming the notion of state sovereignty. Paul Timmers explained how there are three strategies for ensuring state sovereignty in the cyber-space. First, the risk management strategy, meaning to establish cybersecurity through securing critical infrastructure like national electrical grids. Second, the strategic partnerships strategy, meaning only partner with like-minded nations whose values align with yours (for example the 5G debate). Third, the common good strategy, meaning pursue cybersecurity as a common good that benefits everyone.

Timmers, explained that while most countries are pursuing the risk management approach, the cybersecurity as a common good approach seems to be most preferred in conferences like these ones, without a solid governing plan on how to execute it. Catherine Garcia-van Hoogstraten built upon Timmer's strategies by discussing the opportunities and challenges public-private cooperation poses for making cyber spaces safer and more secure. She emphasized one of the strategy's upsides, which is making electronic evidence more available and accessible to public authorities in cases of cybercrime, even when the crimes span over several jurisdictional boundaries.

Panellists also discussed the shortage of cybersecurity expertise. Jacques Kruse Brandao highlighted this by stating 'we are missing cybersecurity experts; everybody is looking for the same people ranging from governments to businesses.' More resources need to be directed to training and educating new generation of cybersecurity expertise. He also highlighted the need to bring cybersecurity as a topic to different faculties in academia, and encouraged inter-disciplinary approach for universities and vocational schools, 'it is not only the engineering students that need to learn about cybersecurity, it's also the marketing, and management domains that need to be educated so that the responsibility for cybersecurity is spread across roles within organizations'.

Chris Painter echoed by stating that 'cybersecurity is still too much of a boutique issue — while it should be mainstream, high-political issue'. He explains that more people in various fields should be addressing cybersecurity challenges, as the challenges span from security to economy to social sphere. Similarly, Arda Gerkens from the Dutch Parliament explained her concern for politicians' apathy towards addressing cybersecurity threats 'maybe we should just sit back and do nothing and let the whole thing explode and then maybe few more politicians will stand up and recognize the problem'.

Catherine Garcia-van Hoogstraten noted that in 2019 the World Economic Forum ranked cyber-attacks among the top five global risks, which demonstrates that cybersecurity is being recognized as increasingly critical risk in the world stage.

Jaroslaw Ponder concluded the panel by emphasizing how important is to help those countries with limited cybersecurity preparedness and commitments in order to raise the common, global standards for cyber safety.

Appendix

In this appendix you will find articles of various speakers and panel members of the 2019 Summit. The content is the sole responsibility of the individual contributors.

Click on the tekst to go to the according article

AUTHORS

AUTHOR
Clementina Barbaro

POSITION
Co-Secretary of Ad Hoc Committee on Artificial Intelligence

ORGANIZATION
Council of Europe (CoE)

Ensuring accountability through regulation

Ongoing work of Council of Europe on artificial intelligence, including on a legal framework on the design, development and application of artificial intelligence.

Ensuring the emergence of a responsible and accountable artificial intelligence (AI) holds a prominent place in the current debates on AI. According to a study published by ETH Zurich[1] concerning ethical guidelines for AI drawn up worldwide, responsibility features at position n°4 amongst the most quoted ethical principles for AI[2]. Responsibility encompasses, in the different texts, the concepts of accountability, liability and acting with integrity.

Ethical guidelines have grown exponentially over the past years. If they represent no doubt an important attempt to identify essential requirements in the design and development of AI applications, it remains that they have inherent limitations: they are not binding and their effective compliance by the issuing organization cannot be checked. Studies[3] have shown that ethical principles have, in an overwhelming majority of cases, only a declaratory nature and are not accompanied by an oversight or enforcement mechanism. It is therefore necessary to go beyond ethics to ensure real accountability.

The Council of Europe (CoE) has taken steps in this direction by establishing, in September 2019, the ad Hoc Committee on artificial intelligence (CAHAI), which is entrusted, within its two-year mandate, with examining the feasibility and potential elements of a legal framework for the development, design and application of artificial intelligence, based on CoE standards on human rights, rule of law and democracy. These standards are not optional for the 47 CoE member states, which are all bound by legal obligations under different treaties: the best known being the European Convention on Human Rights (ECHR), equipped with a unique mechanism of supervision of the respect by member states of the rights and freedoms set forth in the ECHR.

The working methods of the CAHAI will be transparent and open to inputs from civil society and observers, in compliance with the obligation to perform a broad multi-stakeholder consultation clearly set out in the CAHAI Terms of Reference.

During the 1st plenary meeting in Strasbourg on 18-20 November 2019, CoE member states indicated that the feasibility study should include a mapping of legally binding and non-binding legal frameworks on AI, as well as of risks and opportunities arising from the development, design and application of AI. This should be done with a view to detecting possible gaps and identifying accordingly applicable principles to the design, development and application of AI.

Attention should also be paid to coordinating with existing or ongoing work with other international Organizations, in particular the European Union and the OECD, in order to promote synergies and avoid any duplication.

It should be underlined that a possibly binding legal framework establishing a global benchmark, based on human rights, the rule of law and democracy (like Convention 108+ on Data Protection[4]) would not represent a threat to the competitiveness of companies or hamper the development of AI applications. On the contrary, by providing a predictable, homogenous framework for business operations (instead of a variety of ad hoc patchwork solutions) it would increase trust in, and raise the market share

→ AUTHOR
Clementina Barbaro

of, AI applications in line with this framework. Lastly, and fundamentally, such a framework would increase the protection of individuals — at all stages of the design, development and application of AI.

The CAHAI will build upon the important specific sectorial work on AI which has already been carried out by the CoE in different fields. It should be recalled in this respect that the CoE **has the most soft law instruments** of all international organizations[5], reflecting the **holistic approach** that the CoE has taken in respect of AI. From a substantive point of view, the CoE has not simply considered the impact of AI on individual fundamental rights: its analysis has covered, in a broader way, the opportunities and challenges arising from the development of AI for the society as a whole and for democratic systems. As the case of Cambridge Analytica has shown, minor human rights violations can lead to a serious destabilization of our democratic systems and of the electoral processes.

The CoE has already provided concrete guidance to **its member states on how to address these new challenges effectively**, and on the steps they need to take to maximize opportunities and minimize risks. Recommendations addressed to member states with a view to ensure real accountability include carrying out human rights impact assessments on a regular basis, establishing oversight mechanisms and effective remedies and suspending the use of AI applications which are problematic from a human rights perspective[6].

The CoE has demonstrated in the past to be a pioneer in the field of bio-ethics, data protection and cybercrime. The CoE was quick to propose a framework for biomedicine when scientists succeeded in cloning a sheep for the first time in 1996: even today, the Oviedo Convention, opened for signature in 1997, remains the only binding international legal instrument for the protection of human rights in the biomedical field which prohibits human cloning. The CoE is now ready to take up the important challenge of AI regulation, in line with its fundamental values: human rights, rule of law and democracy.

1 Anna Jobin, Marcello Jenca, Effy Vajyena, Artificial intelligence:
the global landscape of ethics guidelines, Nature Machine Intelligence of 2 September 2019.
2 Other principles very often quoted are transparency, fairness, beneficence and non-maleficence, protection of privacy and personal data, respect for autonomy and freedoms, trust and sustainability.
3 See Algorithm Watch, Automating Society: Taking Stock of Automated Decision-Making in the EU.
4 See the Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (CETS: 223).
5 Amongst the most important texts adopted by the Organization the following are featured:
- The Recommendation 2102(2017) of the Parliamentary Assembly of the Council of Europe about Technological convergence, artificial intelligence and human rights
- The Declaration on the manipulative capabilities of algorithmic processes — Decl(13/02/2019)1, prepared by the CDMSI/MSI-AUT
- The Recommendation of the Commissioner for Human Rights "Unboxing artificial intelligence: 10 steps to protect human rights".
- The guidelines on AI and data protection drawn up by the Consultative Committee of the Convention n°108 — T-PD(2019)01

6 See the CoE Commissioner for Human Rights' Recommendation on: "Unboxing artificial intelligence:
10 steps to protect human rights"

AUTHOR
Peter Batt

POSITION
Director General for Digital Society, Digitization of the Administration and Information Technology

ORGANIZATION
Federal Ministry of Interior, Building and Community, Germany

How to bridge the gap between Digital Technology and Legal Frameworks

What are the (21st century) tools and recommendations (both in concept and concrete examples)

First it is necessary to establish that it is not necessary and on the contrary even extremely dangerous to create new legal regulations for every new development that a society undergoes. For any given nation, it is paramount that the government and the law are reliable anchors of stability — the basis for the trust that is the major binding force for every community.

To achieve this legal framework have to be as abstract as possible; they must represent the underlying basic values and political and societal decisions. The interpretation of the law is then up judges who will rule in the light of the law's intent and they will consider new developments like digitization.

That being said it becomes clear that only fundamental challenges to the existing legal frameworks should be addressed by new regulations. Since the changes are happening blindingly fast it is also not advisable to hunt after every symptom that digitisation produces. We need to be as fast as possible without losing the aspiration to provide stability. Therefor we will need room for experiments. New regulations may offer the possibility to test new technology in a confined environment for example. In addition, a new legal framework could have some sort of expiration date, which would force the government and the administration far more effectively than any evaluation program to reconsider what they decided in the first place.

To give a concrete example: Berlin Südkreuz is a railway station that was a testbed (in several areas but also) for facial recognition systems. All citizens knew that and even if the systems was only tested with 275 volunteers such a test could be expanded to possibly cover all citizens using the station the argument being that anyone who is not ready to be part of the test could use another station. Currently the law does not allow for such large-scale pilots. But as we are all facing the "internet of everything" it may become necessary to go beyond traditional means of abstract test methods to explore where and to what extent regulation is necessary and algorithms can be controlled and checked.

AUTHOR
Irakli Beridze

POSITION
Head

ORGANIZATION
UNICRI — United Nations Centre for Artificial Intelligence and Robotics

The Hague Summit for Accountability in the Digital Age was a great opportunity to discuss international policymaking in the fast-changing digital world!

Scientific progress is yielding new technological tools that can deliver great benefits for society. Artificial Intelligence (AI) in particular, is having a worldwide impact on many sectors — from healthcare to finance. AI could even help us to achieve the 17 ambitious global goals world leaders have set in the 2030 Agenda for Sustainable Development. We should, however, exercise a great care and effort in multilateral policy-making and cross-disciplinary cooperation to discuss the legal and ethical implications of the large-scale use of AI.

To access the positive power and potential of AI, we must first work towards ensuring its use is responsible, taking into consideration principles such as respect for human rights, justice and rule of law and requirements such as of fairness, accountability, transparency and explainability.

Accountability is an essential requirement that needs to be taken into account when developing and deploying AI systems. For example, the accountability of automated decision- making systems is one fundamental question to be considered by law enforcement. In order to enable effective legal protection, law enforcement agencies must be able to provide an explanation of an individual decision, and not just the logic involved, which can prove difficult in these systems. In case of an unfair or incorrect decision who should bear the responsibility for the harm done? Engineers and the assigned users in the law enforcement community would be uncomfortable working with such system, for which they could theoretically be held individually responsible. These cases show the need for clear liability regulations in order to reduce the public risks that AI may pose.

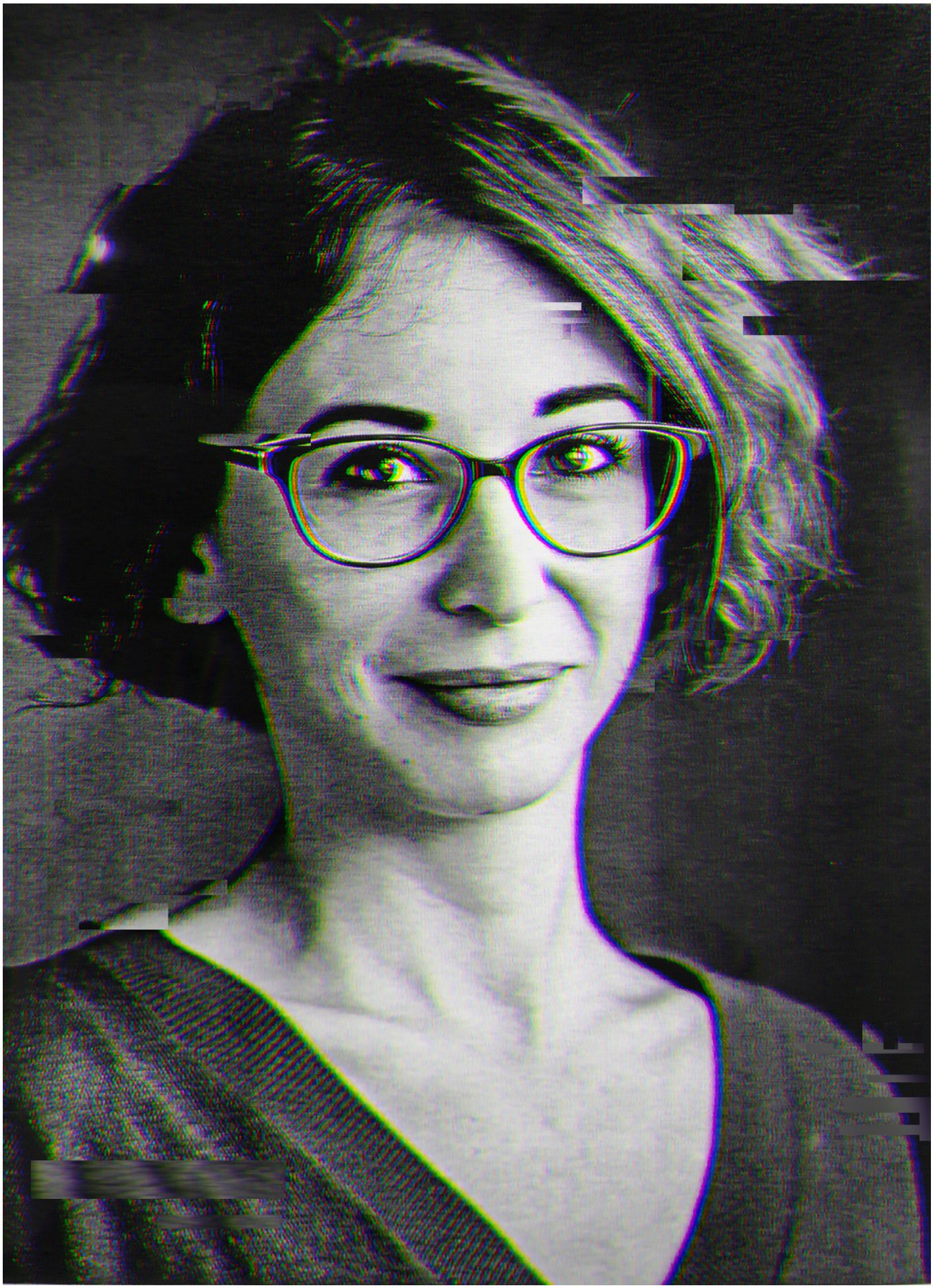
Although there are some early deliberations on national or international regulations, we are still far from creating real international governance mechanisms. Technological advances are happening faster than our ability to respond and, if governments cannot keep pace, they may fall into a practice of prohibiting or banning in an event to minimise the risk that come with the use of AI. However, these approaches may restrict technology development and stifle innovation. How to translate numerous international discussions in concrete policy frameworks and how to create a universal applicable charter will remain a challenge for us to solve.

At the United Nations Interregional Crime and Justice Research Institute (UNICRI), we have established a specialized Centre for AI and Robotics and are one of the few international actors dedicated to looking at AI vis-à-vis crime prevention and control, criminal justice, rule of law and security. We seek to support and assist national authorities, such as law enforcement agencies, in understanding the risks and benefits of these technologies and exploring their use for contributing to a future free of violence and crime.

In terms of AI governance within this specific domain, we have created a global platform together with INTERPOL to discuss advancements in and the impact of AI for law enforcement. Starting in 2018, we organize an annual Global Meeting on Artificial Intelligence for Law Enforcement. The products of these meetings,

→ AUTHOR
Irakli Beridze

which include a joint report in 2019, represents a contribution to advancing the AI governance panorama in the law enforcement community. In connection with the third edition of the global meeting later this year, we will be elaborating a toolkit for responsible AI innovation by law enforcement that will contain valuable guidance and support for law enforcement in developing, deploying and using AI in a trustworthy and lawful manner.



AUTHOR
Dr Berenice Boutin

POSITION
Researcher in international law

ORGANIZATION
Asser Institute

Beyond AI Ethics: International Law and Human Rights for AI Accountability

As AI is progressively being deployed in various public domains such as healthcare, energy, welfare, border security, criminal justice, law enforcement, or defence, we must ensure that the development and use of AI technologies are guided by core democratic values and subject to legal mechanisms of accountability. To this end, established norms and processes of international law, in particular international human rights law, have an important role to play.

In recent years, the sharp advances of AI capabilities have been accompanied by a growing recognition of the need to proactively reflect on its societal implications, so as to shape the development and applications of technology in line with ethical values. Public and private institutions alike have called for a fundamental questioning on the potential impacts of AI, in order to steer AI research and policy towards beneficial outcomes, and to ultimately maintain agency over the technologies we decide to adopt.

The unfettered deployment of data-driven policy-making and algorithmic decision-making in the public sector can indeed come at the cost of many negative consequences, in terms of discrimination, privacy, due process, transparency, and accountability. For instance, the use of risk-assessment algorithms in the judicial system has led to blatant discrimination in the United States, and automated detection of welfare fraud is being litigated in the Netherlands in the SyRI case. The potentially promising and seemingly less controversial applications of AI for example to improve healthcare or energy management should as well be the subject of close reflection and scrutiny, as they are not exempt from risks and concerns.

In this context, sets of guiding principles for ethical AI and informal codes of conduct for self-regulation have proliferated. While the global efforts to reflect on AI ethics are laudable and necessary, it is time to move beyond AI ethics and towards binding legal frameworks and enforceable regulation of AI. It is not to say that new laws are needed: on the contrary, policy and regulatory efforts should primarily seek to interpret and implement existing legal frameworks.

In order to advance AI accountability, international law has a two-fold role to play. First, international law provides for established, globally agreed, actionable and enforceable standards — in particular within the human rights framework, which embodies values such as fairness, equality, dignity, and individual autonomy. Second, international institutions and processes are an ideal forum to debate and engage with possible grey areas and unsettled questions. The international legal dimension does not supplement — but complements — ethical and technical approaches to AI accountability. It is together that the ethical, legal, technical, and policy aspects must be addressed in order to achieve accountability in relation to AI.

AUTHOR
Jeff Bullwinkel

POSITION
Associate General Counsel and Regional Director of Corporate, External & Legal Affairs for Europe

ORGANIZATION
Microsoft

It was a great honor to be invited to speak before a truly remarkable group of policymakers, technologists, business leaders, journalists, and researchers in early November at the Hague Summit for Accountability in the Digital Age, which was sponsored by the Institute for Accountability in the Digital Age (I4ADA). At a moment when concerns about the potential negative impact of social media, artificial intelligence, and cyberattacks are growing, the Hague Summit, with its focus on ensuring that the internet is safe and its benefits available for all, couldn't have come at a more important or opportune time.

Few things have changed people's live as much and as quickly as the internet. In the span of less than three decades, it has become an essential conduit for communications and information, a critical platform for business, a primary catalyst for innovation, and today, it connects nearly 4 billion people to an entire world of ideas and opportunities. Without it, so much of what we take for granted in the 21st century — streaming media, online shopping, GPS directions, the ability to work from anywhere, and so much more — would be impossible.

But for all the benefits that it has delivered, the internet has also provided new outlets and opportunities for cyberbullying, cybercrime and cyberwarfare. Addressing these threats is one of the great challenges of the digital era.

I focused my talk at the Hague Summit on the issue of digital peace. The inescapable truth is that cyberspace is more than just a place for communications, commerce, and content — is it also a new battlefield and we are in the earliest stages of a new arms race.

How significant is the risk? We found out on March 12, 2017, when hackers working for the North Korean government launched the so-called WannaCry ransomware attack. Before it was halted, more than 200,000 computers in 150 countries had been affected. In the UK, more than a dozen hospitals were forced to close and nearly 7,000 people were forced to cancel medical procedures. It would have been much worse if a researcher hadn't more-or-less accidently discovered a way to shut it down.

Then, a month later, a second cyber-attack disrupted significant portions of Ukraine's civilian infrastructure — including the electrical grid — before spreading to computers around the world. The cost to Maersk, the Danish shipping and logistics line, was estimated to be as much as $300 million.

Chillingly, both of those attacks were carried out using cyberweapons developed originally by the U.S. National Security Agency that had been stolen and then leaked by a group of malicious hackers known as The Shadow Brokers.

Now, as we move to a world in which every thermostat, air conditioner, traffic light, vehicle, medical device, hospital, and power plant will be connected to the internet and the security of each of these things will be no stronger then the weakest link among all of them, protecting the safety of civilian infrastructure is more urgent than ever.

There's no doubt that the private sector has a critical to role to play. As part of our focus on creating powerful digital tools that enable individuals and organizations to be efficient, more productive, and more successful, we

→ AUTHOR
Jeff Bullwinkel

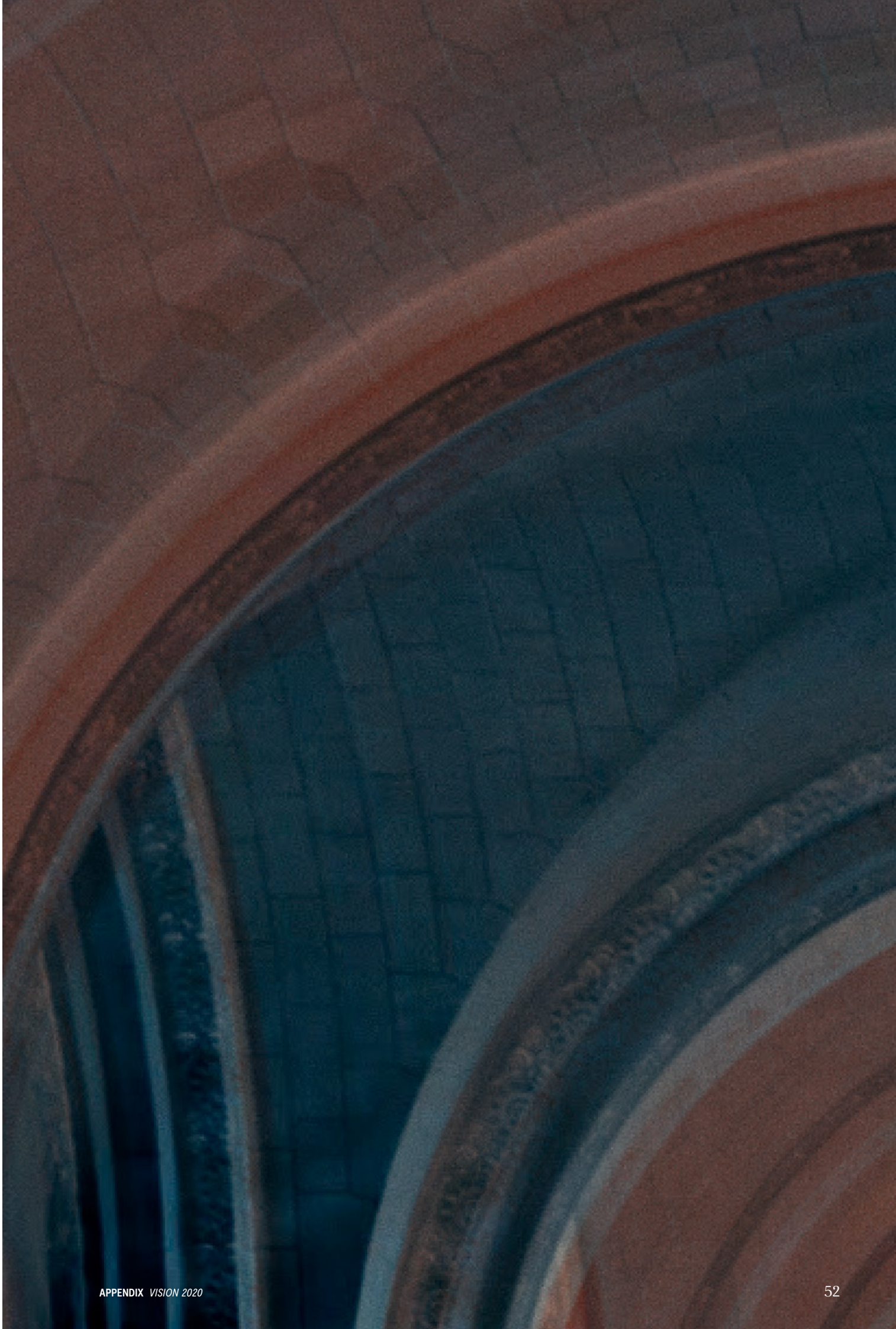
must acknowledge that we have an important responsibility to prevent others from turning technology tools into weapons of war. The good news is that dozens of technology companies have signed on to the Cybersecurity Tech Accord and the Charter of Trust, two prominent industry-led cybersecurity initiatives that include significant commitments to protect civilians and promote cybersecurity.

But a lasting and meaningful digital peace will take more than this. As nations continue to build and stockpile cyberweapons and nation-state cyberattacks continue to increase, it's clear that governments have a critical role to play as well.

The Geneva Convention offers a good model for how we can move forward. Adopted in 1949, it established standards of international law for protecting civilians during times of war. What is needed now are new norms and new international agreements to protect civilians from the risks and dangers of cyberwarfare during times of peace.

Forging a global consensus is no small task, of course. It will require lots of hard work and difficult discussions involving governments, businesses, and civil society. And while we are not there yet, significant work is underway through initiatives like the Paris Call for Trust and Security in Cyberspace and the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online. Both are supported by large numbers of governments, companies, and civil society organizations.

The I4ADA is also at the forefront of the effort to promote global discussions about the establishment of norms for the internet that will promote safety and strengthen accountability. The I4ADA's **Hague Charter for Accountability in the Digital Age offers a compelling starting point for such discussions, and gatherings like the Hague Summit are a critical part of the process to move forward. I look forward to being a part of future discussions sponsored by the I4ADA, as we all work together to create a more secure internet and a safer world.**



AUTHOR
Christina Caljé

POSITION
CEO & Co-founder

ORGANIZATION
Autheos

How to bridge the gap between Digital Technology and Legal Frameworks

As CEO of a media technology company, my contextual reference for accountability in AI is predominantly on core technical and ethical risks, such as explainability, system biases, credibility and deep fakes.

When looking at through a universal governance prism, the absence of specific legal frameworks becomes the key and immediate risk to resolve. Decisions are increasingly made by autonomous AI-based systems, and the existing mechanisms of accountability are not translating neatly to the digital world.

As the pace of AI adoption accelerates across geographies and industries, so does the urgency to evolve our legal system to address the resulting accountability gap. That said, we must strike the right balance between speed and inclusivity in executing this foundational step towards creating accountability for AI systems.

Personally, I see a sector-based approach as most effective in bringing quick alignment on the perceived moral, social and economic risks and potential solutions in cases of 'AI gone wrong'. It's important to recognize that not only will the applications of AI vary per sector, so will the spectrum and severity of potential consequences.

To illustrate why this would be the right path forward, let's analyze the varying dynamics of similar AI techniques applied in two different sectors. Namely, we can compare use cases for computer vision and machine learning algorithms in marketing vs. healthcare industries.

As a marketing use case, I'll reference Autheos since our platform employs both forms of AI in optimizing video marketing strategy for our Brand clients. Computer vision algorithms systematically detect elements such as objects, emotional sentiment and human demographic in our clients' video content. The recognized elements are fed into our data warehouse as output tags and, based on the client use case, those tags are one of the (many) input factors into our performance based machine learning algorithms that autonomously decide which video is shown to a visitor on the client's consumer site.

Besides optimizing the consumer's video experience onsite, interconnectivity between our computer vision and machine learning algorithms facilitates quantitative insights Autheos shares with the client's content team, in order to inform their digital (video) marketing strategy.

Contrasting this with the healthcare context, an AI-system based on computer vision and machine learning has a completely different use case. Computer vision is increasingly used to analyze digital images and medical scans at scale. Combine this capability with a machine learning algorithm that analyzes large volumes of previously diagnosed cases, and you have a powerful tool that can identify complex patterns and make diagnoses that might otherwise be missed by a (human) doctor. We are seeing such AI systems transforming dermatology, radiology and cardiology medical fields.

With these two sector examples in mind, the worst case scenario of AI gone wrong might 'only' result in reputational risks or lost revenue in the marketing example. For a marketeer, this downside scenario might feel disastrous but, it pales in comparison to the potentially life-changing or, in extreme cases, life ending effects in the healthcare use case of AI.

→ AUTHOR
Christina Caljé

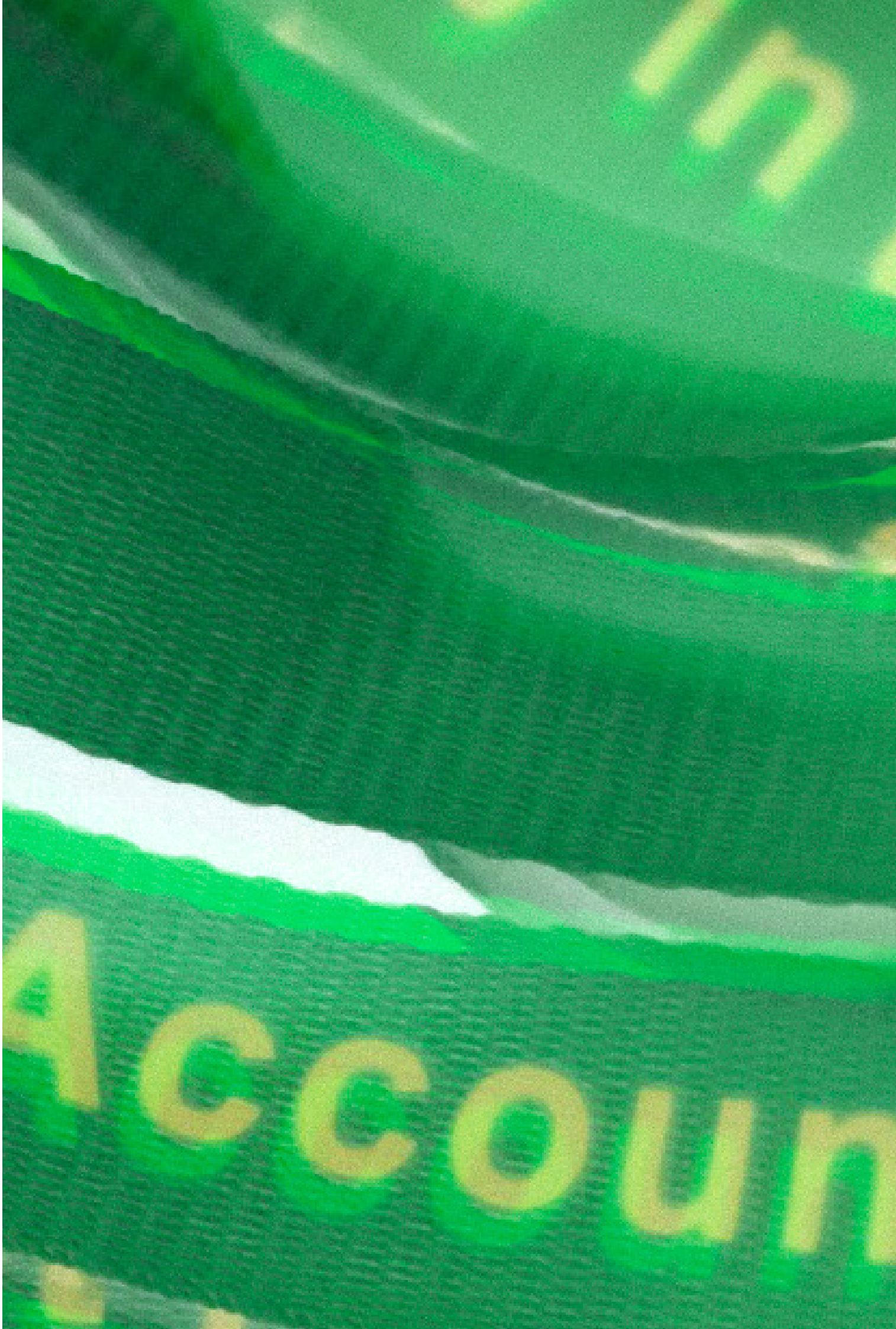
With such wide ranging applications and downside risks across just two industries, aligning multi-industry stakeholders on the most urgent risks to tackle seems an almost impossible task, let alone establishing a full legal framework in the immediate term.

Instead, the aforementioned complexities necessitate a new and iterative approach towards policy making in this digital age. Establishing a preliminary legal framework, created and overseen by a global stakeholder group of industry experts would yield a first, quick win towards regulating AI and defining accountability.

In selecting the stakeholders per industry to spearhead these sector based initiatives, it's crucial to adopt an inclusive approach that extends beyond the obvious choices. Since innovation is global, diverse representation from continents and companies of varying stages of maturity - startup to scale up to publicly traded company - will enrich the perspectives and help to 'future proof' the eventual frameworks.

After preliminary sector-based frameworks are in place, a network of international agencies should take the next step, scanning and identifying foundational similarities to build upon. The 'battle-tested' industry frameworks will deliver learnings to inform a v.2 overarching framework spearheaded by the international agencies that eventually replaces or complements the sector-based initiatives.

This sector driven approach will allow us to not only move quickly, but also to yield a flexible solution that maintains relevance and effectiveness as the applications and implications of AI continue to drastically alter the world we live in. This would be a new strategy to policy making, but as society is evolving in this digital age, so too must our approach to governance.


Account

AUTHOR
Joelle Casteix

POSITION
Founding member of the board of directors

ORGANIZATION
Zero Abuse Project

A bad actor spreads false information, disguised as news. As a result, large populations ignore the risk of a fast-acting virus, refusing vaccinations and disregarding quarantines. Within months, a global pandemic kills millions worldwide.

A biotech firm creates apps that make life easier for millions of people by storing their health and biological data. The firm sells that data to marketers, who then exploit that information. In addition, bad actors within the firm funnel medical information to rogue third parties, who create false identities to file fake insurance claims and purchase big-ticket items.

A security firm creates an algorithm that claims to predict behaviors that will target potential criminals. Law enforcement nationwide purchases the product, which unknown to them, was created with systemic and unintentional bias that targets specific vulnerable populations.

A multinational bank creates a strategic partnership with a social media giant for marketing and outreach. Because of weaknesses in their third-party product, hackers gain control of the banking information of millions of corporate clients, resulting in financial collapse.

How would you react? What should we as a global society do?

These situations are not hypotheticals. Instead, each of the above scenarios is a real threat in the digital age. What can we, as thought leaders, global businesses, NGOs, government bodies, and individuals do to stop current threats. How do we create a world where accountability across digital platforms is rigorous, enforced and preventative? And how can we accomplish this and not stifle creativity and entrepreneurship?

Should we treat the Internet as if it is a "Wild West"? Even the creators of the Internet disagree. Why is it that the vision of its earliest creators is now marred by the differing visions of the current state of that technology?

Is it up to the creator of a technology to monitor its progress? Or is it up to the users of that technology to create a structure that guides further iterations of that technology?

These are the questions the Institute for Accountability in the Digital Age (I4ADA) addressed at its latest summit in The Hague as they continue to address and construct guidelines, strategies and framework for global digital accountability. The credibility of the Internet and our digital information is at stake.

Whos and Hows

Now that we have determined that there is an ethical, legal, and technological imperative for greater accountability across all digital platforms, we must consider who we are protecting and why is the integrity of these audiences and their data is important:

The Vulnerable — Vulnerable people, whether vulnerable due to socio-economic status, age, education level, location, governmental structure, war or famine — anyone without power is in a position to be exploited.
Privacy — Personal privacy must be a high priority.

→ AUTHOR
Joelle Casteix

The Rights of Content Creators — Without guaranteed protections for content and technology creators, innovation is seriously jeopardized.
Data and Information integrity — Following privacy, data and information integrity are tantamount. Fake news, deep fakes etc., must be addressed and stopped at their sources.

How

Now that we know the "whos," how do we create a framework for digital accountability? The first consideration is Rule #1: Accountability dies in compromise. Any structure of framework put in place must create and maintain high standards that are not "diluted" by committee, compromise, or power imbalance.

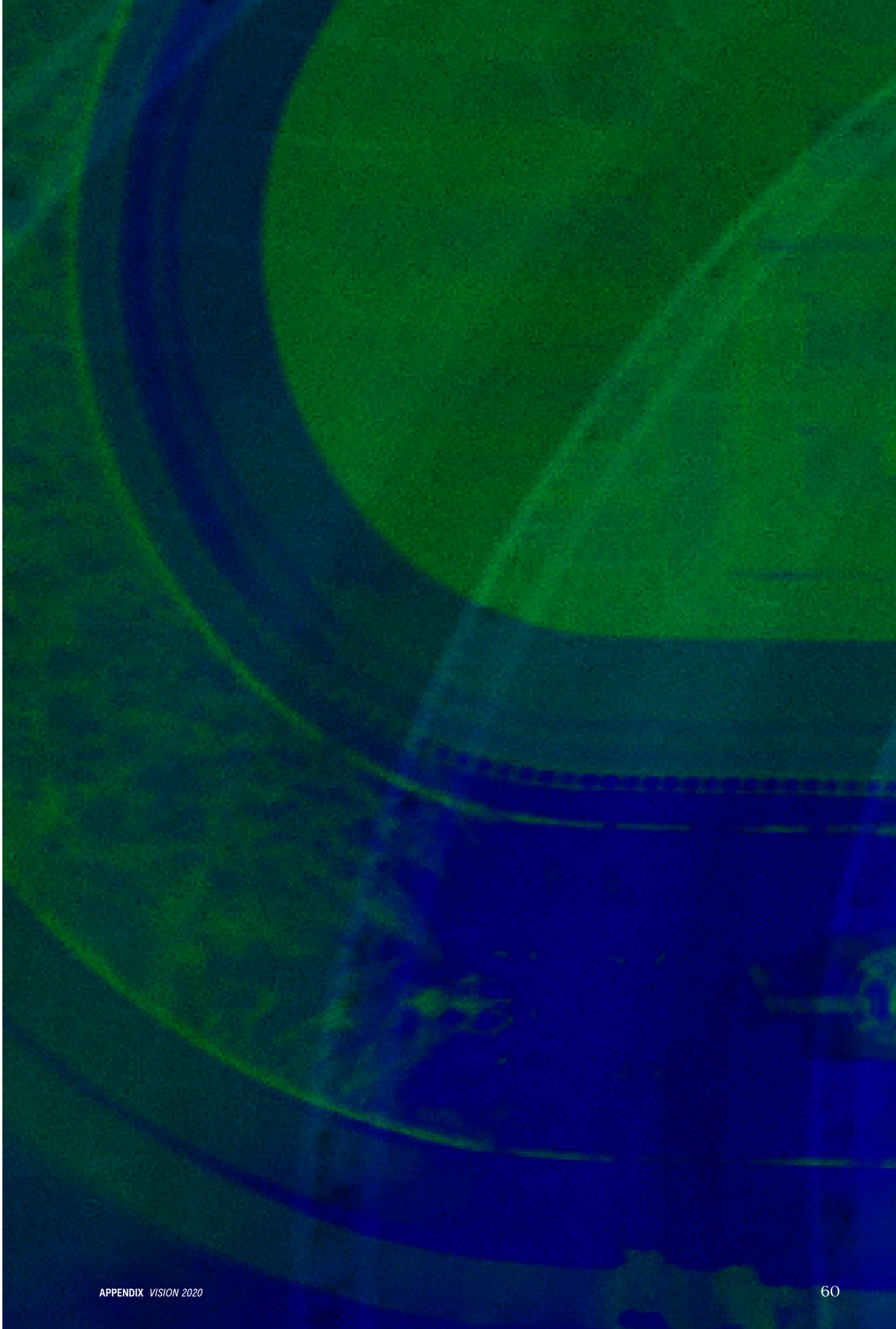
Therefore, we must consider the following:

Equity - Those in positions of power must not be able to use that power to threaten access or integrity of the digital information of less powerful individuals.
Rigor — Laws without teeth are ignored. Corporations and individuals must have strong incentive to act the right way and strong disincentive to act with malfeasance.
Prevent the slow creep — There is a folk saying in the United States: Throw a frog in boiling water, and he will jump out. Put the frog in a pot of cool water and turn on the stove, the water will slowly heat and boil the frog to death. We can use this as a parallel to the "slow creep" of internet accountability. Small compromises and minor slides in rigor, while not life threatening, will slowly and effectually erode the accountability of an entire digital platform.
Culture change — Our current global "laissez faire" culture when it comes to digital accountability must change so that incentive to do good comes with both within and outside of an organization.
Education — Culture change begins with education throughout all levels of society and will be instrumental for creating a world where digital accountability is expected and standard, not the anomaly.

Next Steps

We know the imperative for this upcoming decade is clear. Now, it's time for all relevant stakeholders to come to the table to develop strong international civil and criminal laws, good governance strategies, and economic incentives for compliance and innovation in the digital accountability space.

The I4ADA has broken ground and made huge progress in a short period of time on these issues. But they can't do it alone, nor should they. The time has come for big data, social media giants, ISPs, IT companies, NGOs, news organizations and governments to come to the table and contribute to real change … before malfeasance and corruption create their own rules and regulations.



AUTHOR
Vinton G. Cerf

POSITION
Chief Internet Evangelist

ORGANIZATION
Google

Accountability is a bedrock concept in democratic societies. Without accountability, a society becomes authoritarian in nature and its leadership unaccountable. What should be protection of citizens from harm becomes protection of the State from accountability. At the heart of accountability lies identity. There can be little accountability without the ability to identify the accountable. On the surface, there may appear to be exceptions. Anonymity to protect a whistleblower is a well-established principle, but the credibility of the whistleblower often depends on his or her identify. A credible whistleblower process will establish but then protect that identify.

I would like to introduce a concept I will call "differential traceability." The idea is that while anonymity or pseudonymity may be a surface norm, proper authorities should have the ability to penetrate these facades under the right circumstances such as court orders or standing operating procedures. Automobile license plates offer an example. While license plate identifiers may appear to be random, commissioned police officers have the authority to associate the car's registered owner with the license plate at need. Note this does not associate the car with the driver of the car - only the registered owner. Indeed, a traffic stop for bad driving might reveal that the driver isn't the owner and on subsequent investigation may actually be in the possession of a stolen car.

This same notion of differential traceability has another aspect worthy of consideration. There may be times when it is highly valuable for an individual to be able to "prove" his or her identify. One wants to make it hard for someone to falsely claim to be you - so we turn to biometric, strong cryptographic authentication methods and related measures. Such means are vital for parties to engage in transactions that benefit from both (or multiple) parties being able to strongly authenticate the identities of all transacting parties. A modern example can be taken from the so-called "permissioned blockchain" in which all parties know the identity of the blockchain participants. This knowledge aids in the development of trust in the blockchain. While I am not a big fan of blockchain as the "solution to everything," I favor knowing who the involved operators of the chain are to the anonymous alternative.

If we are to have the ability to conclude contracts across jurisdictional boundaries, we are going to need strong authentication of transacting party identification so as to provide accountability and recourse. Investment in common tools of authentication strikes me as one important element in aid of global accountability.

AUTHOR
Charles Groenhuijsen

POSITION
former US Correspondent

ORGANIZATION
NOS Journaal & NOVA

There is a lot of fake news about fake news. It started about five years ago. Suddenly there was a lot of writing about the phenomenon of fake news. I will be in journalism for about 40 years around that time. And I was surprised.

There were two reasons for me to be surprised. Why were journalists all over the world suddenly so worried about the misinformation and misinformation of humanity? And every time I went looking for research to confirm that it was very serious with the fake news, I was disappointed. I could not find those investigations. Yes, there is fake news, it is becoming more sophisticated, and more and more people are falling for it. This is often a reason for journalists to report prominently and alarmingly. Is that fair? And based on facts?

To begin with, let's get rid of the idea that fake news was invented by malevolent mates, who unscrupulously try to earn a lot of money with it. We should not forget that conscious deception is as old as humanity. Kings and popes, pastors who unscrupulously try to earn a lot of money with it. Let us not forget that conscious deception is as old as humanity. Popes and pastors, politicians and presidents: they have all been guilty of spreading fake news on a large scale for their own benefit. Every time people in power consciously try to inform my believers, subjects, voters or parishioners incompletely, there is fake news.

Let us also not forget that we have had mass media for about 200 years. First newspapers and magazines, then the radio and television, and now more recently internet. The invention of the printing press is now about 500 years ago and has improved the spread of knowledge unbelievably. But for the first few 100 years, the power over that information was primarily reserved for those in power with religious or worldly power. That has been more often a means of suppression than of emancipation. Anyone who now worries about fake news should not ignore that historical perspective.

Journalists have an incurable preference for bad news. The recent surge in fake news is a festive treat for cynical reporters, presenters and opinion leaders who eagerly tell the world that there is cause for great concern about independent journalism. Of course, that malicious fake news is the cause of people being poorly informed. That must be eradicated root and branch.

Journalists are critical. That is a great thing. Those in power must be checked and the press is indispensable. But it is sad that he does not extend his critical attitude of journalism to his own functioning. Journalist research and everything but the consequences of their own work. Let us simply formulate, as far as the goal is concerned, "Optimally informing people about the world around them".

And is that a bit successful? Well, we don't know that much about it because journalists rarely investigate their own functioning. Journalists are critical and that is a great thing. Those in power must be checked and the press is indispensable. But it is sad that journalists do not extend his critical attitude of journalism to their own functioning. Journalists research and everything but the consequences of their own work. Let us simply formulate, as far as the goal is concerned, "Optimally informing people about the world around them".

→ AUTHOR
Charles Groenhuijsen

And is that a bit successful? Well, we don't know that much about it because journalists rarely investigate their own performance. Those in power must be checked and the press is indispensable. But it is sad that journalists do not extend this critical attitude of journalism to their own functioning. Journalist research and everything but the consequences of their own work. Let us simply formulate, as far as the goal is concerned, "Optimally informing people about the world around them". And is that a bit successful? Well, we don't know that much about it because journalists rarely investigate their own performance.

Imagine cardiologists or oncologists who is curious about the results of their treatments. At the exit of the hospital they ask the departing patient: and did you like it a bit? Most patients will be relieved to say that they are very satisfied with the treatment. Glad they can go home again. If doctors examined their own functioning this way, we would laugh at them. It is much more relevant whether those patients are still in good health two or five years later.

Journalists only do superficial research at the exit: the circulation, the number of clicks, the turnover in advertisements. But whether their efforts have contributed to a broad public being well informed about the situation in the world? No clue.

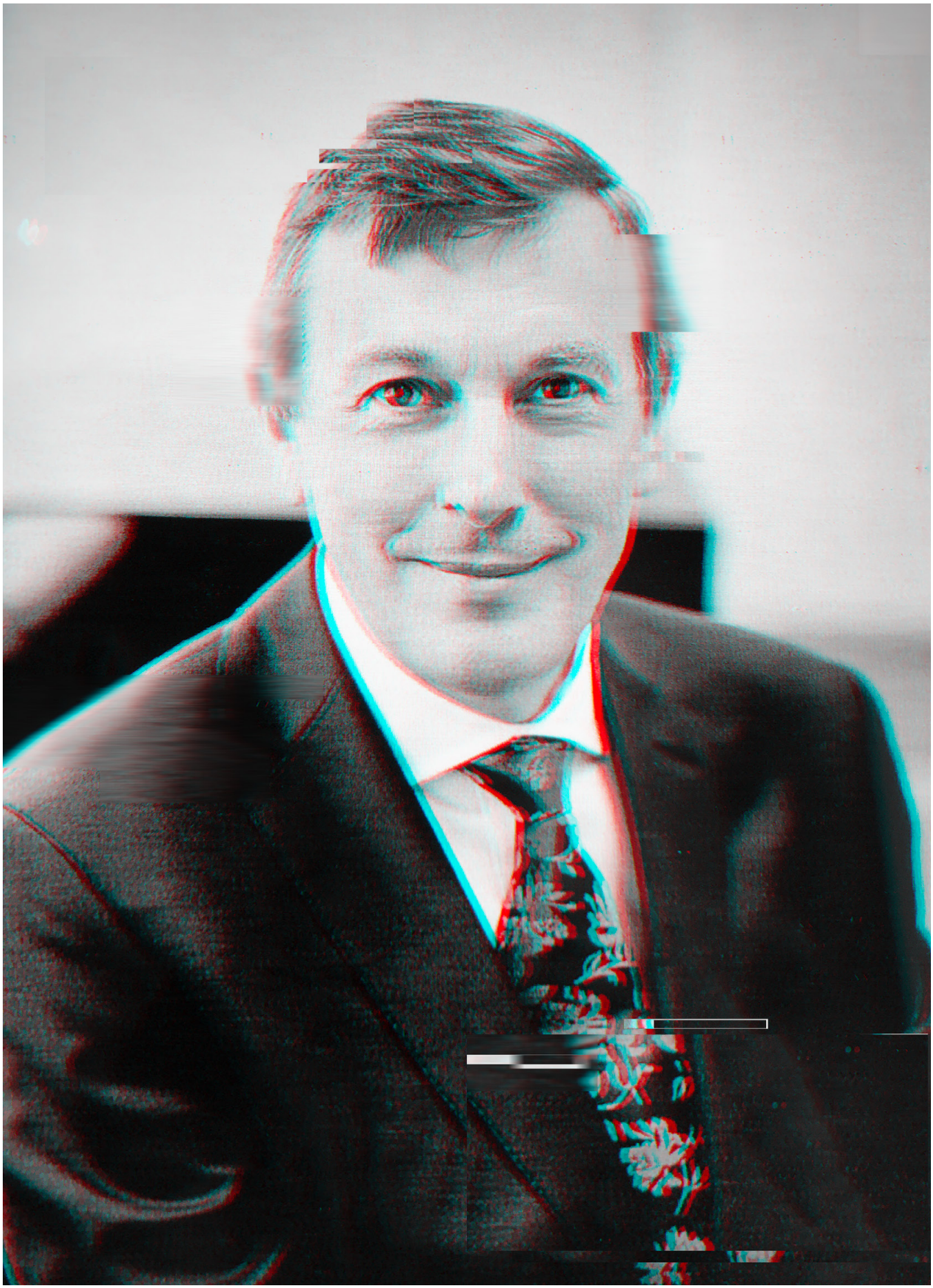
We rely on external institutes for such research. And every time it is clear: the public is miserably informed. Fortunately, a project called The Perils of Perception does such research and comes to this amazing conclusion: “We are wrong about nearly everything. Perceptions are not reality. Things are not as bad as they seem”.

Or take the unsurpassed website OurWorldInData. Founder Max Roser investigates whether **people are well** informed and concludes: “Most of us are wrong about how the world has changed; especially those who are pessimistic about the future. The widespread ignorance about truly important changes in the world feeds into a general discontent about how the world is changing. “More than 9 out of 10 people do not think that the world is getting better. How does that fit with the factual evidence?”

The Swedish researcher Hans Rosling (he died in 2017) examined for many years the visitors to high-end, international congresses. Highly educated, therefore, they are opinion leaders of international politics. But they are, Rosling concludes, suffering from “devastating ignorance”.

And do not forget: There is no fake news involved here. It is the mainstream media that are responsible for this staggering knowledge gap among a broad segment of the news consuming audience. Media mostly ignore progress in the world. Good news is no news, is their adagium.

And that bring us to accountability of the media: if journalists really want to bring the professional goal in life (better informing of the public) closer, they have to look at themselves and sow a little less panic about fake news. Improve the world; start with yourself.



AUTHOR
John Higgens

POSITION
Chair

ORGANIZATION
Global Digital Foundation

Trust me — I'm accountable

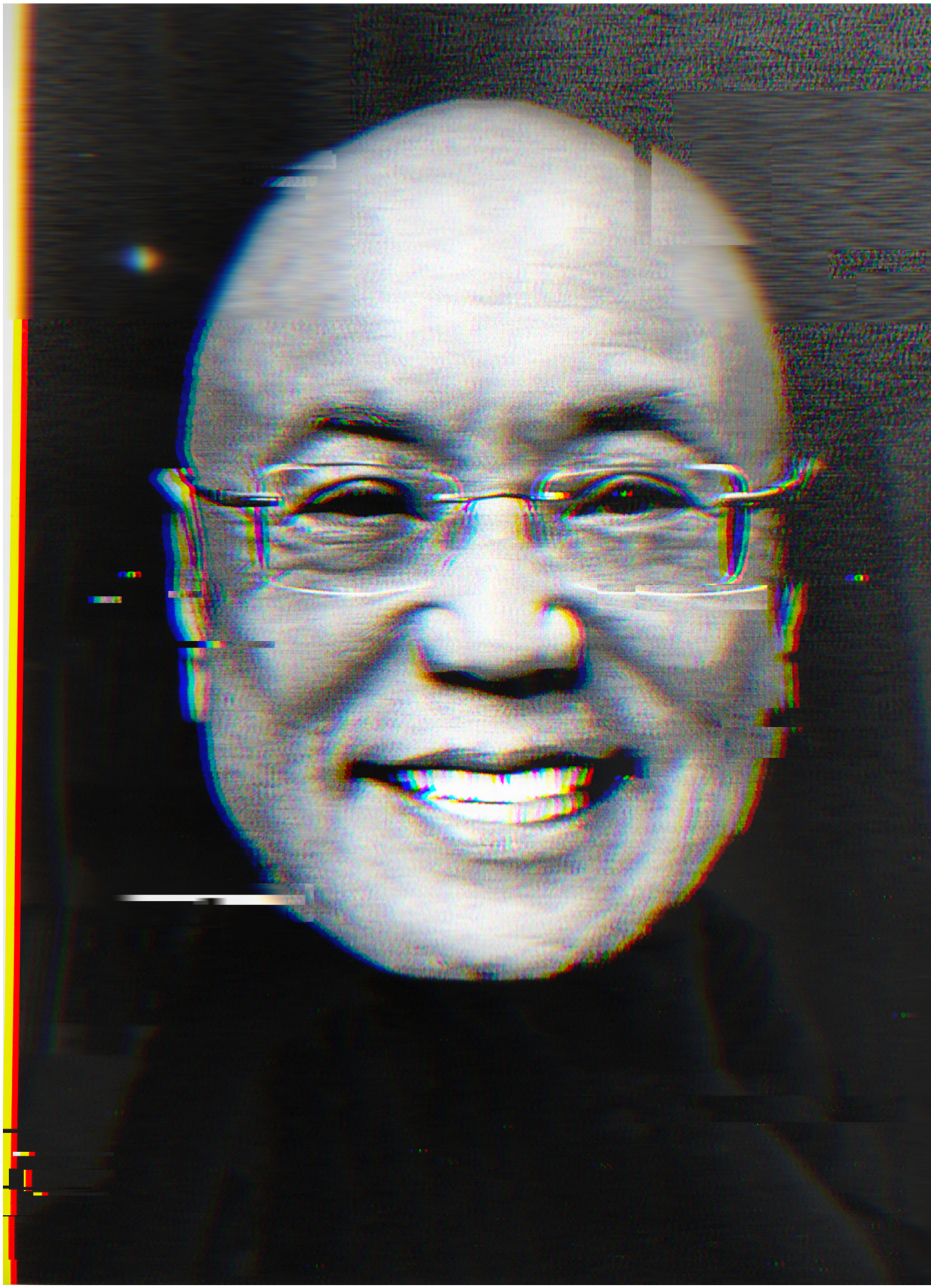
The currency of trust creates value for humanity in the digital age. Society's progress is built on trust and progress falters when trust is called into question, as we saw in the 2008 financial crisis. We learn to trust in a variety of ways, including by the results of our dealings with people and by listening to the opinions of others, and we give more weight to the views of those we come to trust. When people gather in organizations we learn to trust those organizations in the same way — companies work very hard to become trusted brands. It's difficult to persuade people to do business with you unless they trust you.

Accountability underpins trust. Things go wrong in every aspects of life; we all make mistakes. How we deal with those mistakes makes a big difference and this is particularly true when you are operating in the online world. There are countless examples of how to handle it badly; we all know of cover-ups, obfuscation, denials. In the digital age customers are often one step removed and will only keep trusting, and using/buying, if they see transparency and above all accountability. This means both giving an account, (how did the mistake happen?), and taking responsibility — for resolution and redress.

Being in a position to give an account requires an organization to develop a culture of accountability and put in place the right processes and procedures, capturing enough data about transactions, for example, so that when mistakes occur it's possible to go back and understand what happened, how and even why. A culture of accountability helps individuals and organizations learn quickly from mistakes.

The most common form of Artificial Intelligence in widespread use today, machine learning, can make the first part of this accountability — giving an account — more difficult. Explainability is one of the key challenges for producers and users of machine learning. I've heard machine learning developers say [about a specific algorithm] with some surprise "we didn't expect it to do that!" But it's vital that the writers of these algorithms are given the tools and then use them to anticipate and explain how the algorithm reaches its conclusions in clear and simple terms. Without this the transparency/accountability/trust relationship risks breaking down with serious consequences and even loss of legitimacy. This is true for commercial activity but also in the healthcare, criminal justice, and education sectors too.

Machine learning is perhaps simply the latest challenge an accountable organization must deal with. But organizations which understand that accountability underpins trust will master this challenge. These are the companies, enterprises and public bodies that will prosper and thrive in the digital age.



AUTHOR
Stephen Ibaraki

POSITION
industry analyst, writer and consultant

ORGANIZATION
REDDS Capital

I had the great pleasure to participate and speak at the Institute for Accountability for the Digital Age (#I4ADA) Summit 2019 and then to share my insights and recommendations.

There is an immediate need to focus on accountability due to A Triple C. ACCC is defined as an unprecedented time of change where the next five years will determine the course of history for the planet through Hyper:

- **Automation**
- Time **Compression** in new innovations measure in weeks and months
- **Convergence** of the three domains: the physical, digital and biological
- **Connectivity** due to unlimited computational power

Underlying all of ACCC, the 4th Industry Revolution now trending towards Society 5.0 and the 5th Machine Age and the 40 billion IoT and 300 billion interconnected devices.

The changes are so profound that the impacts are observed across: governments, industry, academia, media, civil society, culture — every aspect of the United Nations 17 Sustainable Development Goals (SDGs).

These impacts require: accountability, responsibility, transparency, fairness, ethics, equity, explainability, interpretability, contestability and much more. There are already more than 100 frameworks around accountability which in 2019 are transitioning to operational processes. Examples here are the EU, OECD, Canada, Singapore, Australia, G7 Global Partnership on AI (6 of 7 governments are in support) and global non-profits such as IEEE P7000, ACM Code of Ethics, ISO/IEC JTC 1/SC 42 Artificial Intelligence, IFIP 2020 global code of ethics project. IEEE is the world's largest engineering organization. ACM is the world's largest computer science organization. Founded in 1960, IFIP is the United Nations UNESCO-founded federation of computing organizations. ISO is the international standards organization; IEC is the international electrotechnical commission; JTC is the joint technical committee.
With regards to governments, Canada led early with an AI strategy in 2016 and their findings and processes are freely shared. This is illustrated with the work of Ashley Casovan, past Director of Data and Digital for the Government of Canada, who moved in 2019 to Executive Director of AI Global.

Moreover, it's good to follow the work of David Bray, Executive Director, People-Centered Internet coalition and Senior Fellow, Institute for Human-Machine Cognition.

This is also gaining the attention of CEOs. In August 2019, more than 180 CEOs of the largest companies, indicated publicly that they will equally prioritize the community, and multi-stakeholders and not just shareholder value. Larry Fink, founder of Blackrock, the world's largest investment fund at over US $6 Trillion in managed assets came out publicly in 2018 and 2019 in support of social impact. This is also occurring with the high-net worth, of more than 20 million, who hold in excess of US $60 Trillion, as millennials take over from past generations — with millennials social value is important. This also was reported at Davos last year from the YPO when they conducted an internal survey. The YPO released their seven leadership trends for 2019 and their shift towards social impacts through business from their 2019 Global Leadership Survey.

→ AUTHOR
Stephen Ibaraki

An added example, at the 2019 I4ADA Summit, these CEOs participated:

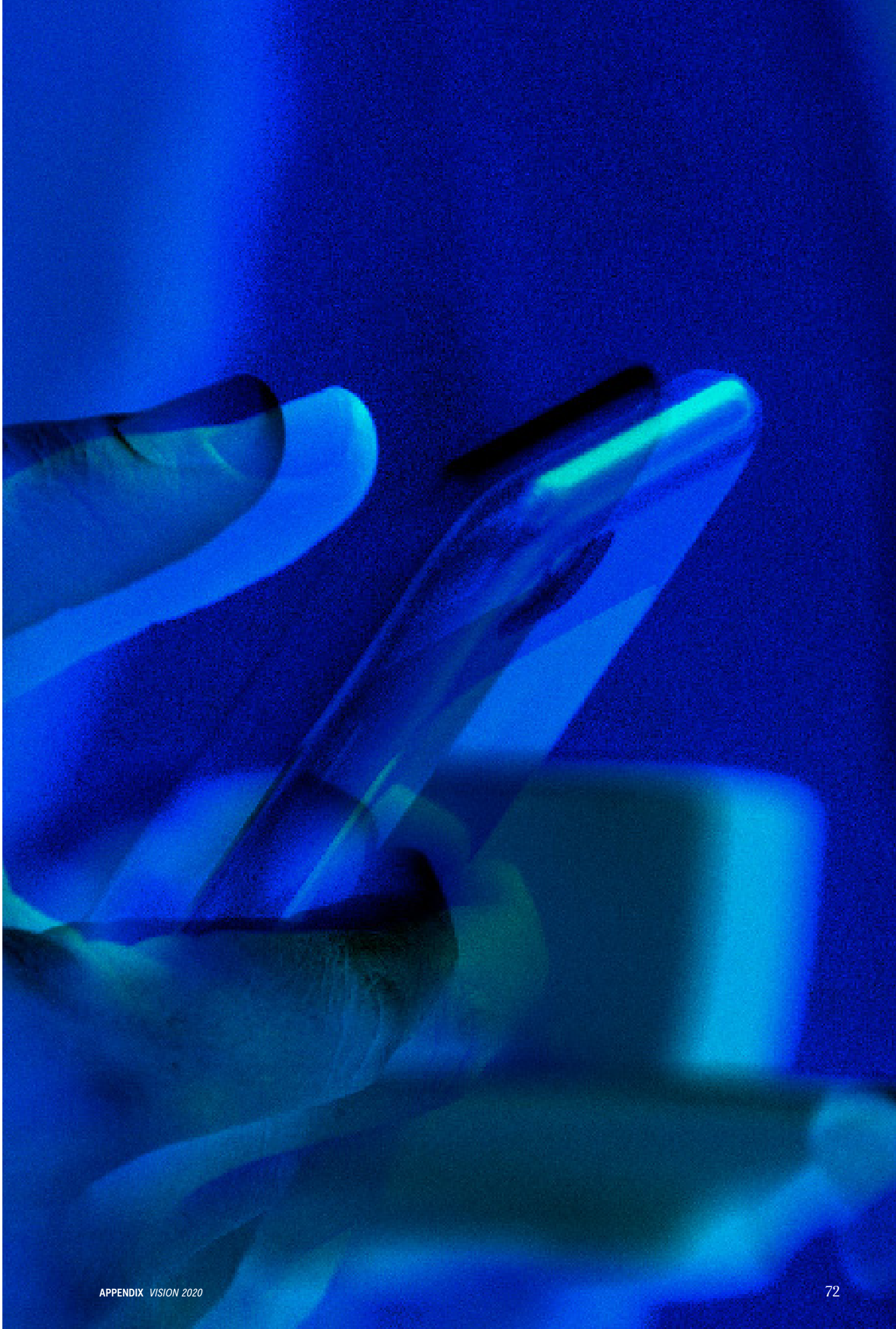
- YPO Impact Network Council Chair / Co-chair YPO EU Impact Summit, Sivaaji De Zoysa
- YPO Co-chair YPO EU Impact Summit / Impact Officer YPO European Region Board, Oleg Volkosh
- YPO European Region Board Chair, Vadim Belyakov

YPO is the leading notable CEO organization: 28K CEOs representing US $9 Trillion annual revenue across 130 countries in 460 chapters. The YPO EU Impact Summit (EIS2020—Oct 19/20 2020) is addressing the world's biggest challenges by execution. EIS2020 would be a first in YPO bringing members across 84 chapters in Europe to jointly select, ideate and collaborate on the 5 biggest issues in impact forums across the region during the year leading up to the event. YPO in a recently concluded survey has identified the top 5 challenges its members want to adopt and solve. These challenges and their relationship to the SDGs are:

1. Environment & Climate Action (SDG 13, 14, 15)
2. Future of the Eurozone (SDG 7, 9)
3. Migration and Refugees (SGD 1, 2, 10)
4. Economy (SDG 4, 8, 9, 11, 12)
5. Cyber security (SDG 16)

EIS2020 would be an international event, with a cap on 500 registrants. It will be an international event given YPO leaders and members from around the world would be interested in conducting a similar summit in the future in their regions. This program is in complete alignment with YPO Europe's Vision 2020 based on three key pillars; collaboration, engagement and use of technology to implement programs, enhance value of their interest-based platforms and use networks as a key channel to members.

Thus accountability is at the forefront led by I4ADA bringing together stakeholders from all sectors.



AUTHOR
Jacques Kruse Brandao

POSITION
Global Head of Advocacy

ORGANIZATION
SGS Digital Trust Services

Accountability & Cybersecurity

2019 was a very active year related to Cyber-security. We did not only see again a growing number of connected IoT devices and services but also new attack vectors which caused huge damage to global businesses. Again, we realized that cybersecurity is an issue we can only tackle together.

The presentations and issues discussed in the panel discussion *Accountability & Cyber Security and Cyber Peace* at the Accountability Summit 2019 showed challenges and gaps we still need to work on in the next years. Those ranged from various angles including predictable and timely consequences for attackers, the possibility to generate cross-border e-evidence to be used in courts while complying with privacy regulation like the GDPR, some interesting aspects why to change from risk management towards collaborative approach and the necessity for cybersecurity capacity building in nearly all disciplines.

Upcoming cybersecurity laws with different requirements being launched in various countries in 2020 may not reflect the need of the industry to comply with related to their products and services for global markets. They also do not reflect yet the necessary requirements to prevent damage caused by state-of-the-art cyber-attacks. Global cyber norms might be a possible solution here. Who can take the lead to define a common denominator of cybersecurity rules? Countries might use for their national cybersecurity framework whatever has been generated in multi-stakeholder processes like the European Cybersecurity Certification Framework currently being filled by ENISA, the European Cybersecurity Agency, together with the European Member States and industry stakeholder. Already the GDPR acted as a blue print for various nations' privacy laws like the CCPA in California or LGPD in Brazil. We will see if the European Cybersecurity Act finally will have a similar role for other jurisdictions.

The OECD and its recommendations for global norms on cybersecurity and on the Protection of Critical Information Infrastructures will also support this approach.

The *Charter of Trust* shows one possible way forward how to secure global supply chains. Global industry players like SIEMENS, NXP, SGS, Allianz, MHI, Telekom, CISCO, IBM and others work together to define and promote Baseline Cybersecurity Requirements and Security-by-Default up to certification for critical systems. Each member of the supply chain focus on securing his domain based on his special expertise like in components, devices, applications, communication, cloud or contribute with related insurance or validation services. It generates a jointly defined set of cybersecurity requirements also to be used as basis for third party compliance testing to generate trust between two business partners.

Governments need to define supporting regulation and policies related to IoT products, services and processes to generate a level playing field that companies will be incentivized when they invest in safety and cybersecurity. This will strengthen not only their industry but also the position of nations in the context of national security and their resilience against cyber-attacks.

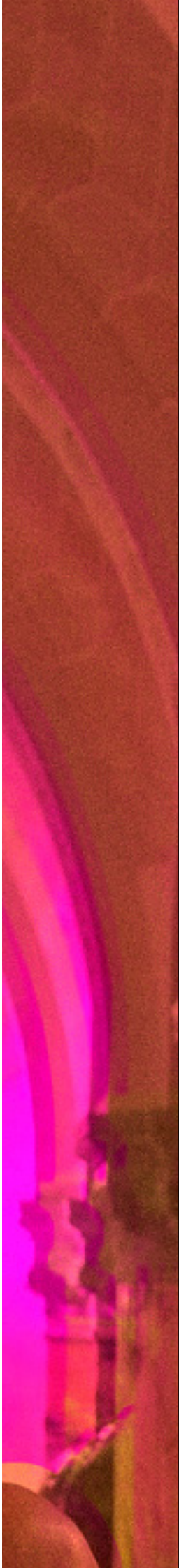
Will voluntary cybersecurity requirements be enough? New use cases like automated and

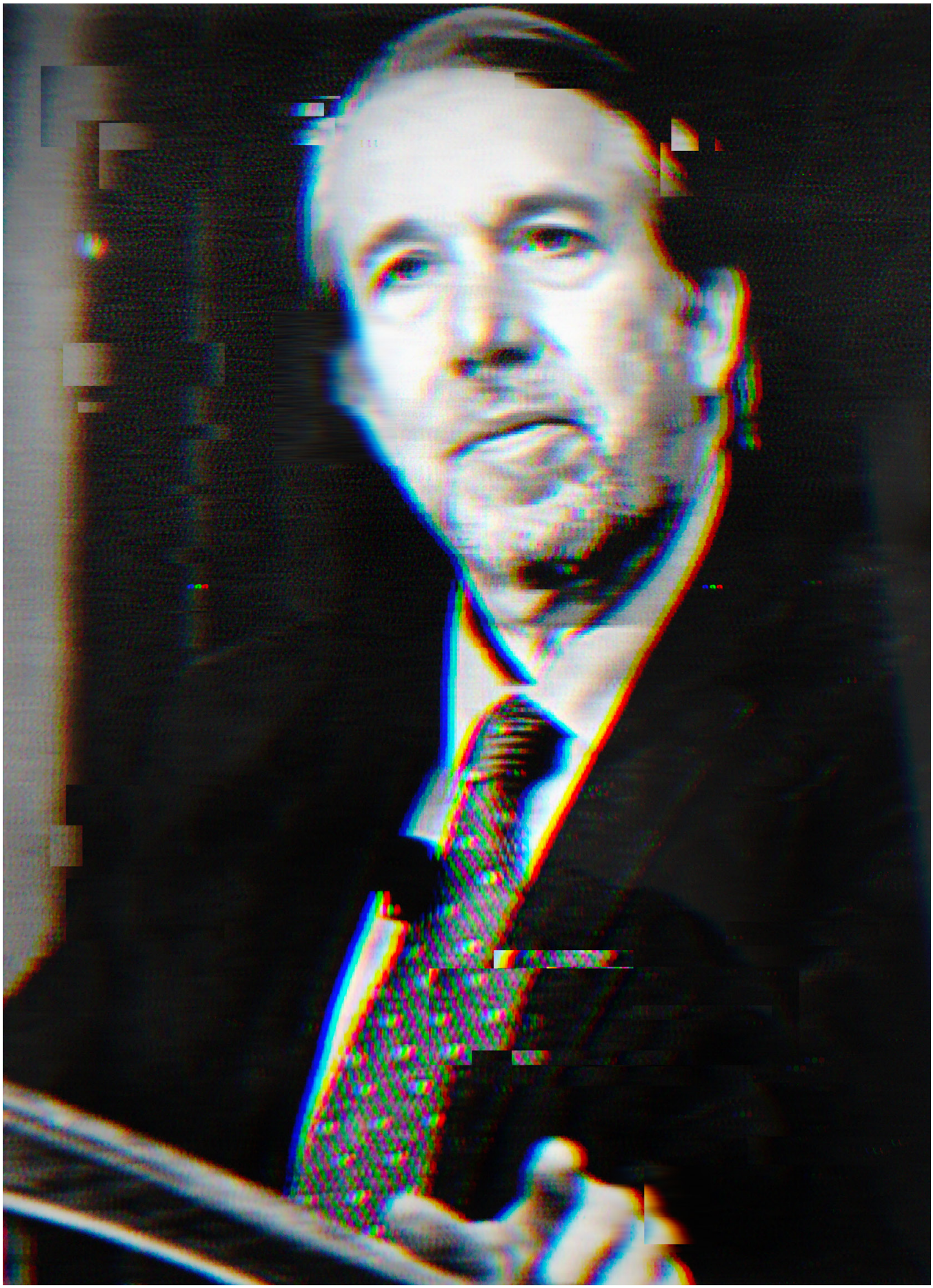
→ AUTHOR
Jacques Kruse Brandao

autonomous driving or flying — I think about flying taxis being part of new mobility solutions and intelligent transport systems in our smart cities — will require additional rules, not only in the U-Space but also from a cyberspace perspective, that people will trust and use them.

To generate trust into disruptive technologies like Artificial Intelligence we first need to trust underlying basic data as well as the criteria to select certain data which is used to generate algorithms for machines to later decide autonomously with effect on human beings. Secure identification of people, devices, data and services will support such selection of data, avoid misunderstanding and generate transparency. Ethical rules for software development like they have been proposed by the High-Level Group of Artificial Intelligence of the European Commission are a first step. Now we need to generate clear KPIs which can be validated by third parties to show compliance to customers, partners and governments before they will become part of the legal framework for AI.

In Europe a quite comprehensive cybersecurity certification framework is now in place. To cope with the expected raising number of connected devices and services in the coming years we need to gear up in speed and fill the cybersecurity certification framework with clear requirements. Only then developers and manufacturers globally understand what is expected and can take the accountability and implement those features accordingly that customer can trust those secure devices and services and gain from the digitized world.





AUTHOR
Chris Painter

POSITION
Commissioner

ORGANIZATION
Global Commission for the Stability of Cyberspace

There are many kinds of accountability in cyberspace but one area that has been sorely lacking is accountability for nation-state large scale malicious cyber conduct. Although the international community has made good progress, and even has secured some key agreement, on certain "norms of behavior" for state actions in cyberspace, without any accountability and consequences for those that violate those rules of the road, they end up being little more than words on paper.

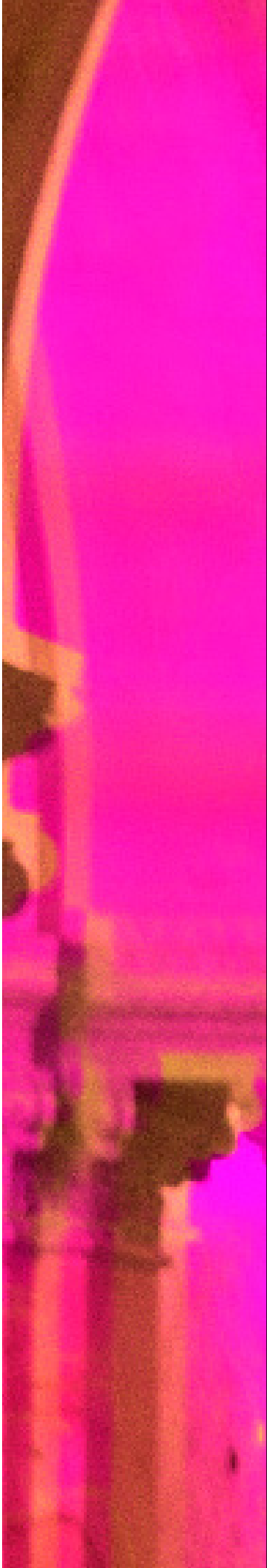
Countries have agreed in the United Nations that international law applies in cyberspace and have agreed on certain "norms of restraint" and cooperative measures. For example, countries have agreed to a voluntary norm against conducting cyber-attacks against the critical infrastructure of other countries in peacetime. That is an important development that, if observed, would substantially bolster the stability of cyberspace and allow all the positive things that computer networks bring, including social inclusion and economic growth, to flourish. Nevertheless, over the last several years, there has been a seemingly ever increasing number of malicious cyber events of ever ascending severity and impact. The Not Petya worm attributed to Russia caused a significant amount of damage to infrastructure including international shipping. The WannaCry worm, attributed to North Korea, caused international damage including effectively shutting down the UK's National Health System.

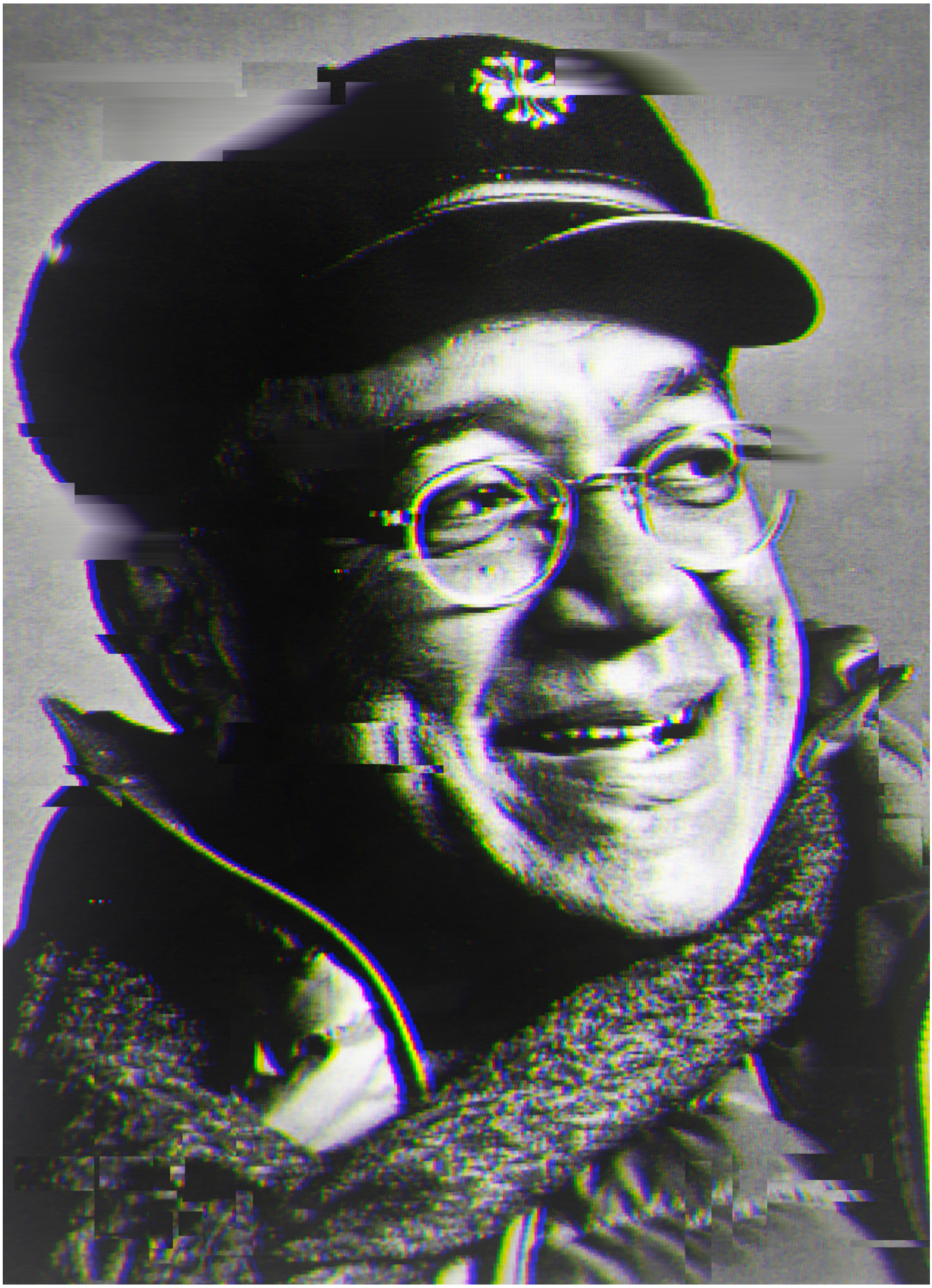
Yet, against this increasingly dangerous backdrop, too little has been done to hold bad actors to account. When the actors are criminals, there has been an increase in international cooperation to make sure that those actors are arrested and prosecuted. While much more needs to be done to strengthen cybercrime laws, investigations and prosecutions, at least the path forward is reasonably clear. There has also been some progress in collectively calling out bad nation-state cyber behavior. In both the Not Petya and WannaCry cases, a number of countries came together to announce joint attributions. While calling out such bad behavior is a good start, in both cases, it was many months after the fact and its impact was lessened. Moreover, there are a few actors where "naming and shaming" is ineffective and where such public attribution must be followed by actions that impose appropriate consequences on bad actors both to sanction them for past conduct and deter them from future malicious activities. The global community has not been good at either collectively or individually imposing appropriate costs for bad behavior and the actions taken so far have been piecemeal and not strategic. Instead of deterring such behavior, this lack of action has only emboldened such actors to engage in such activity again. Worse yet, other potential bad actors on the sidelines observe the lack of any true consequences for bad action and it encourages them to join the fray.

For there to true accountability for malicious cyber activity we must do better. There are some hopeful signs that we are moving in this direction. The EU recently approved a "Cyber Diplomacy toolkit" that allows EU sanctions for malicious cyber activity. The US is carrying forward a cyber deterrence strategy designed to act collectively with other countries to counter malicious state sponsored activity. The Global Commission on the Stability of Cyberspace, among other things, has recommended that both state and nonstate actors work to ensure that "those who violate norms face predictable and meaningful

→ AUTHOR
Chris Painter

consequences." We must all work together to bolster these budding accountability mechanisms, while ensuring that the consequences we impose are themselves are understood and not escalatory. Only then will long term stability be ensured either in the cyber or the physical world.





AUTHOR
Cyril Pereira

POSITION
Media Consultant Asia

Why promote digital transparency & accountability?

We are in the Disinformation Age of high-speed news channelled by AI programs to targeted individuals and groups. Social networks form cocoons and bubbles within which such content goes viral. Both extreme right and left of the political spectrum, are similarly boxed. Society gets polarized and dysfunctional.

We have no 'silver bullet' to kill misinformation and disinformation. State and non-State actors employ digital technology and social platforms to push their political and commercial agendas. The Big Business-Government nexus sponsors political parties. The private sector funds ruling elites for mutual benefit.

Only supra-national institutions can be effective in the borderless 'digital commons.' The Hague hosts the International Court of Justice. It also has the *Institute for Accountability in the Digital Age* whose remit goes beyond content distribution, to include the regulatory authorities and technology companies. All the players need to interact, to devise effective solutions.

Useful steps toward a 'global commons' service

- → Framework a verification matrix for all content to identify author, source, location, and trace archive of content generated from host sites
- → Develop a rating system for authors and sites with colour-codes for trust, and flag authors and sites which are unreliable, or malignant
- → 'Follow the money' to identify ownership & funding for sites and authors
- → I4ADA can work with Regulatory Authorities and the Digital FANG giants, to establish a baseline international standard on content integrity
- → Provide training for Ombudsmen to handle complaints on content deemed false, malignant, or inciting hate. Train and support country chapter leaders of i4ADA
- → Publish a regularly updated list of unreliable sites and authors. Publicize and encourage editors and journalists to contribute verification
- → Document fact-checking sites for news content by region and country
- → Collaborate with international institutions:
  - · Knight Foundation
  - · Poynter
  - · Pew
  - · International Fact-Checking Network
  - · Lead Stories
  - · Digital Forensic Research Unit/Columbia Tow Centre
  - · Stanford Internet Observatory
  - · The Reporters Lab/Duke University
  - · PolitiFact, etc.

Should State actors be invited?

As the speed and chaos of fake news explodes, States are passing laws to bring online content into the same legal framework as print publishing. A balance has to be struck between legitimate criticism of governance and fake news. Sometimes that is not the case: invoking such laws may be a cover for totalitarian information control.

This tendency to impose laws on digital content creators and publishers can only multiply, in the absence of a universally agreed set of parameters. It will be useful for i4ADA to invite States which have already passed internet content laws, to share. Other States can benefit from the models. An opportunity to review such laws would benefit those who have positive intent.

→ AUTHOR
Cyril Pereira

It will be productive to invite the PRC which has increasing influence over Africa, the Middle East, and South America, as a major infrastructure investor in the developing world. Their telecommunications and mobile networks are part of the infrastructure upgrade. The ITU (*International Telecommunications Union*) is already a partner with i4ADA, for this to work.

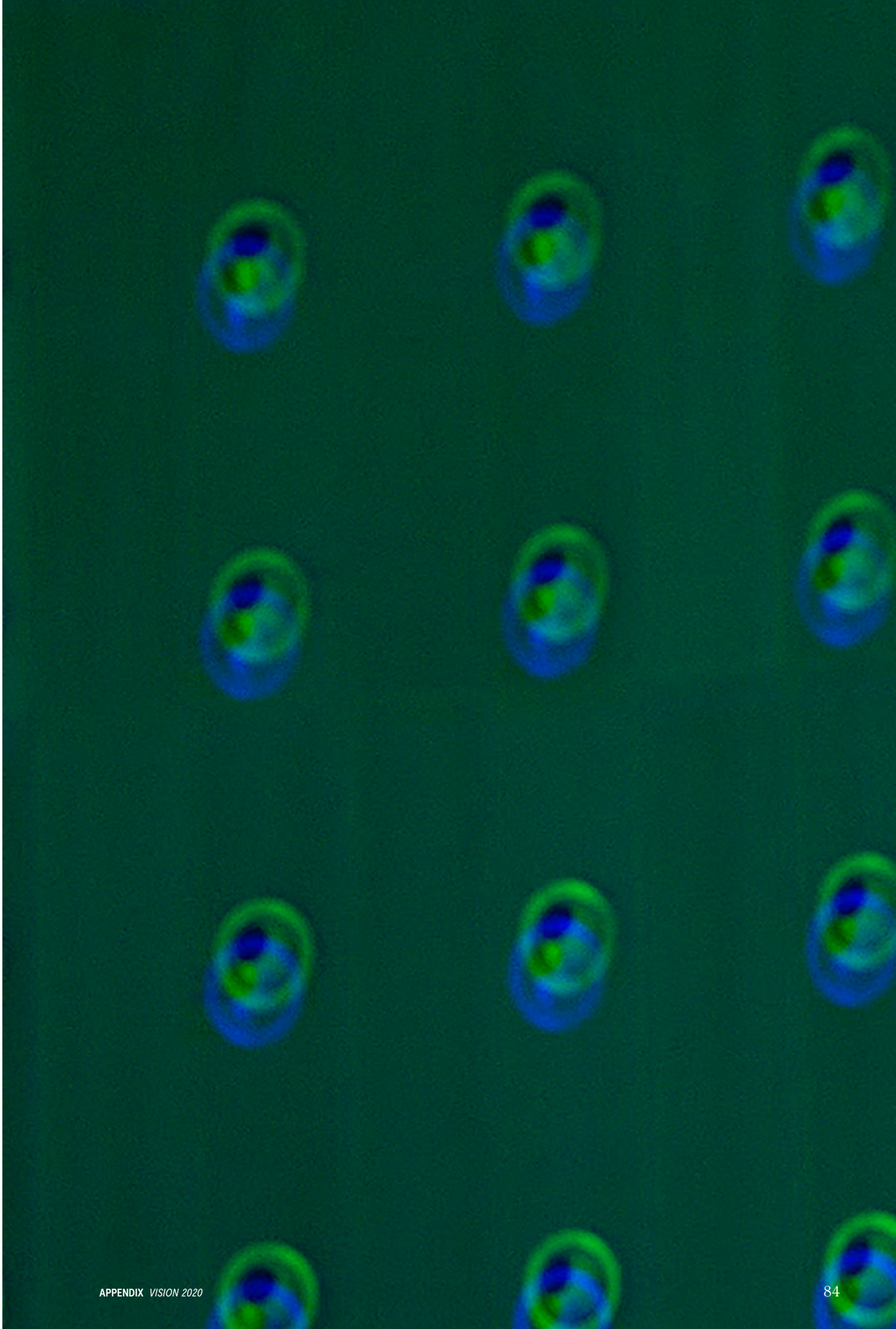
Should FANG be present at the i4ADA Summit?
Facebook, Amazon, Netflix & Google are the giants facilitating the bulk of digital consumer flows. They are the primary global platforms for social interaction, e-commerce, entertainment and email/search. They write the AI programs, vacuum the personal data, monetize identity, track users online and via GPS, and stream content.

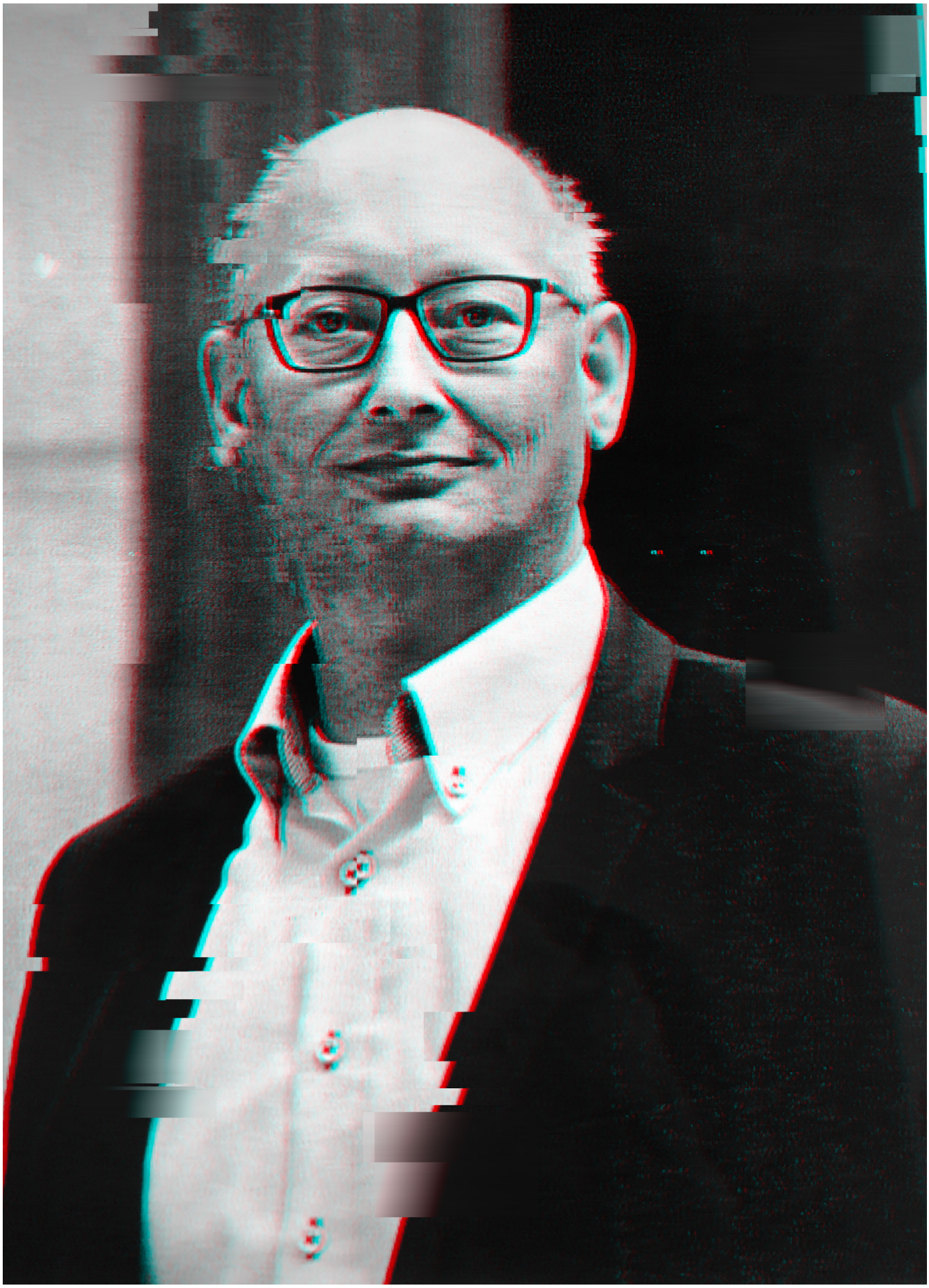
Only by making FANG transparent and accountable, can the issues of privacy and abuse of secret data, be managed. They are critical to the quest for a responsible, human-centric internet. They can also be tapped for joint studies and project funding. They have a major stake in the regulatory frameworks, which can impact their business.

Tap the experts, speed up the rectification
It may be productive to engage key stakeholders in dedicated sessions within the Summit program, for consensus to act. The i4ADA should be a facilitator to solve the known problems rather than another forum for venting. It has stakeholder goodwill. The Hague has a respected track record with the ICJ. I4ADA can leverage that to nudge the stakeholders positively.

There is no need to wait for the perfect 100% solution. The dangers in the digital chaos need immediate rectification — an 80% solution is useful now. It can always be refined once in place. Agreed solutions need to be put into place as practical models, for adoption by countries and digital enterprises.

Make panels informative
Domain experts are information-rich. That is the value for the audience. Just having them appear but blocked from sharing deep insights due to time curbs, does not serve the audience. Delegates appreciate solid content and new information. Smaller panels at 8-minutes each allow for meaningful sharing. Effective moderators, and speakers who prepare, deliver value.





AUTHOR
Lukas Roffel

POSITION
Chief Technology Officer

ORGANIZATION
Thales Netherlands

Due to the future reality of a world largely depending on AI and autonomous decision making systems, as a global supplier of critical systems we have a strong interest in the alignment of laws and regulations. Because in many of our applications human lives are at stake, transportation, aerospace and defense, the impact of these laws and regulations, especially on the humanitarian part is important.

At this moment we are always considering humans to be an essential part of the decision making process. However in a growing number of applications the human operator is becoming the weakest link in the process. Although creativity is still a strong advantage of humans, in a growing number of cases algorithms, rules and learning systems can outperform a human. We already see this in aerospace and transportation applications. We therefore need a new framework within which to operate. This shall be a discussion on a global scale, but like in other topics like privacy, we can also start this in a smaller community to make faster progress. This may be necessary also because we do not all share the same standards and values as societies.

We believe that this new framework needs collaborative work between countries, governments, knowledge institutes and companies to be able to have a committed and supported solution. And this solutions needs to be adaptive since we are only at the beginning of the changes to be brought about by AI.

We should especially be aware that all around the globe not the same standards and values are adhered to and therefor a smaller group may start an initiative rather than to start as a UN working group. We are willing as a corporate enterprise to participate actively to this discussion and to come to a solution in the shortest possible timeframe.

We also need to consider in these discussions that boundaries within which AI shall be defined. Also a standard for the quality of the data, data ownership and for which purpose the data is used, needs to be part of (or parallel) discussion around AI. Without this a bias in autonomous systems cannot be managed.

We need a framework that is simple enough to result in trustable AI — everybody should live without fear because AI is **Tr**ansparent, **U**nderstandable and using **E**thical standards — TrUE AI.

AUTHOR
Andrew Taussig

POSITION
Former Director of Foreign Language Services

ORGANIZATION
BBC

The 2019 Summit was successful and stimulating — but was, by virtue of its very success, also a wake-up call to the challenge of defining valid and realistic principles for an accountable and democratic internet. The very word 'internet' conjures up something tangible and physical linking a myriad of www's of web-linked addresses — like some physical cable or chain which can be cleaned, scrubbed, polished, sanitized, covered with masking tape, rendered totally safe, even beautified. Presentations and discussions in the Hague shone a bright light on the cold and complex reality that for us, as human beings, the internet is not a single' thing' but a range of different experiences, scenarios and arenas inseparable from the different domains where individuals or groups of users live and work. What they initially turn to as a tool becomes an end-in-itself, transformed according to context into a series of distinct scenarios with differing interests, experiences and expectations.

1. The internet, for the journalist - working freelance or otherwise - may be the platform of choice for personal projection, as news reporter, trend-watcher, blogger, debate-leader, controversialist, caller-out of fake news and disinformation, dis-entangler of narratives and counter-narratives, often involving fake/pseudo/junk/hoax news
2. For the business leader (Microsoft, Thalys) it may be the medium ideally suited to ideas- and data-sharing, a pathway to a best practice code which brings manufacturers, distributors and retailers alongside insurers, accountants and other industry professionals.
3. For the AI specialist it may serve as a rich evidential source for ways of injecting human intelligence or even 'empathy' into AI and for validating safety certification in proposed AI applications or devices.
4. In terms of movingly human scenarios, the Summit heard about the capacity for the internet to drive (especially) adolescents to dangerous addictions (e.g. gambling and video-gaming) and to physical self-harm or even suicide; but alongside it were examples of the Internet's capacity to intervene constructively, so sufferers and family members could use the internet to 'bounce back' Those, for example, whose particular passion is preventing and penalizing sexual or other social abuse discover in the internet a degree of personal redress, an effective alarm system, and a methodology for tracking criminal behavior and reaching out to victims.
5. In the field of cybersecurity, whether combatting freelance hackers or nation state attackers, defense and related specialists tend, like Clausewitz, to see cyber-warfare like traditional warfare as the continuation of diplomacy by other means — with cyber-peace and cyber-security being the only ultimate guarantee of a safe world.
6. From those involved in the work of the International Criminal Court and comparable jurisdictions came a sense of frustration that it was proving so much more difficult to define and establish criminality inside the index of cyberspace than it had been to reach consensus around war crimes and genocide.
7. The teachers and academics on the panels brought a keen awareness of how the digital internet had transformed the tool-kit of the learning environment and - along with the toolkit - the pupil's or student's view of the world and their potential or aspirations within it.

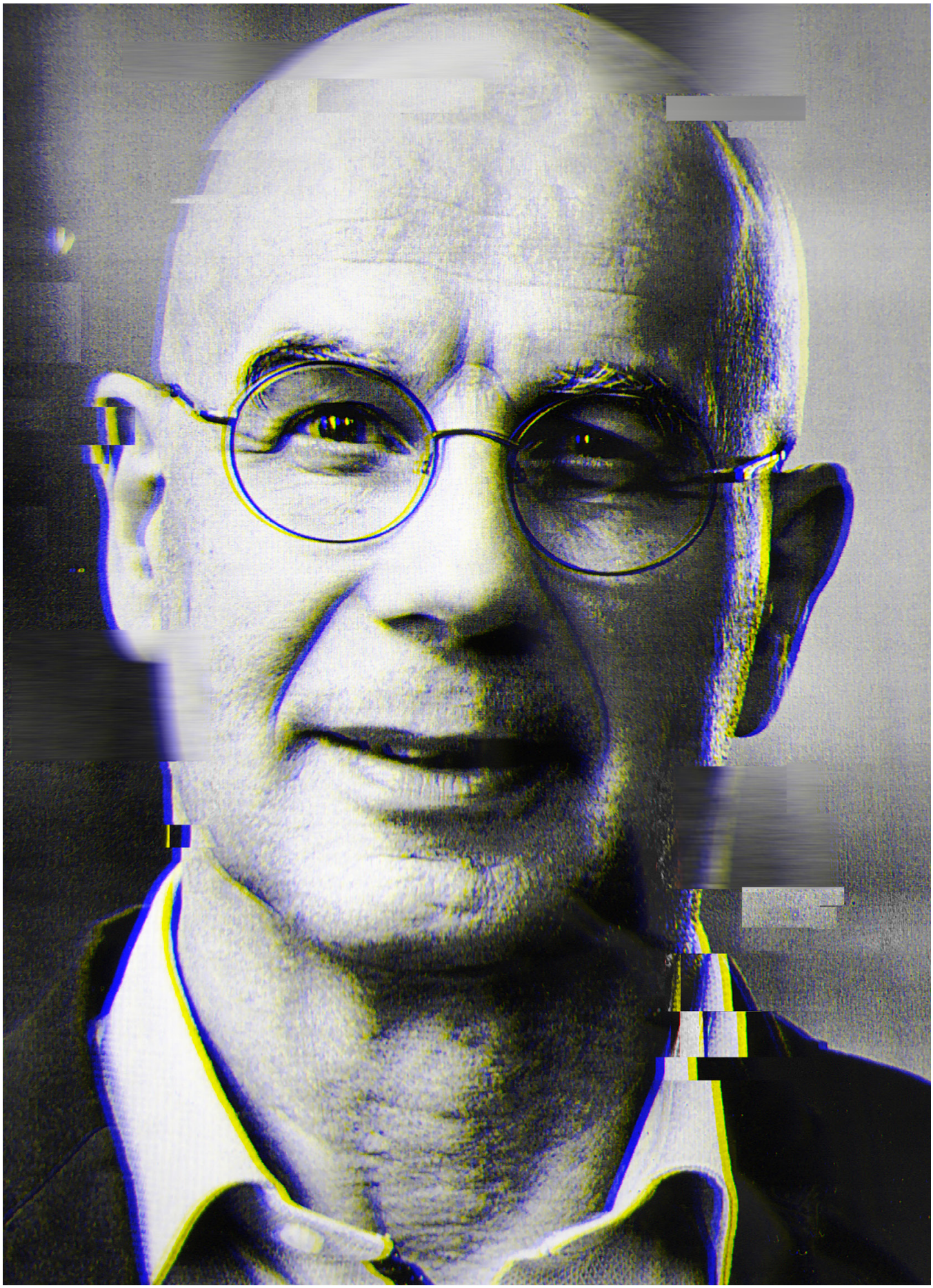
→ AUTHOR
Andrew Taussig

8. Lastly perspectives offered by representatives from international or supra-national organizations [UNESCO, ITU, Council of Europe and EU reflected the dilemma at the Summit's core: of striving to straddle the range of differing concerns and capacities applicable to their various member states — the likely axiom being that the larger the membership the more difficult their task and the greater, therefore, necessary skepticism about a "coalition of the willing" approach, based on existing national enforcement agencies, which may however leave less well-resourced stakeholders stranded as non-participants or de facto bystanders.

Whilst formulating standards, and delivering accountability for being compliant, presents a problematic challenge, useful first steps can be made through identifying the desirable attributes of a decent and democratic internet. An immediate proviso needs adding: that such attributes may, indeed will, find themselves in competition with each other [for instance privacy versus responsibility and accessibility versus anonymity], requiring balanced, 'lesser of two evils' types of judgements consistent with the overall aim of an ethical and accountable framework seeking a reasonable balance of rights and duties for members of the global internet community. Allowing for such limitations or reservations, the Hague Principles could call for and endorse an Internet which is...

- ✓ **Open**, because the web enables entry to, and content exchange within. the public information/communication domain for billions who otherwise would not have such access and can benefit from the potential which the internet offers for enhanced human contact, education and capacity building
- ✓ **Safe** from intrusion and harassment driven by commercial (especially fraudulent), social and sexual motivation, as well as from unmonitored exposure to such online temptations as gambling and videogaming
- ✓ **Prohibitive** of unacceptable items as hate speech, homophobia, images of child abuse and acts of extreme violence or terrorism
- ✓ **Privacy-protected** from data-gathering, including by official agencies accessing personal information beyond what is reasonably required on grounds of state and societal security
- ✓ **Transparent**, so that anonymity may not be used, on free speech or other grounds, to evade identity-tracking nor privacy arguments abused by individuals or 'closed' groups to impede intervention from regulatory bodies, platform operators and others who legitimately curate websites — thereby sabotaging the regulation of the internet
- ✓ **Compliant** with democratically established regulatory codes in so far as they embody and enforce standards which support an ethically accountable internet and are compatible with relevant United Nations instruments such as the (2015) R.O.A.M Principles for Internet Universality
- ✓ **Technology neutral**, encouraging innovation in digital devices and software (e.g. in the field of Artificial Intelligence or The Internet of Things) thereby promoting creative collaboration among specialist practitioners and users at all levels within the global online community, pursuant to the goal of a democratic and adequately accountable internet.

SHORT NOTE I feel there is missing here an attribute/adjective relating to *editorial responsibility*; but I can't quite work out what would be right or realistic. As Cyril points out in his video-contribution, there is no recognized editorial framework or reference point across the internet. Only a handful of the billions who post on the internet are, in any real sense, editors. Nor do they, indeed, need to be. Content deficiencies vary from the inaccurate and imprecise to the malevolent and the libelous/slanderous. The rules about carrier responsibility for content are in flux. Draft legislative proposals abound. The consequences of 'bad' content may be anything from almost zero to serious personal harm or reputational damage; and judgments about legally justified compensation or broader consequences for 'victims' will be equally unpredictable and variable.



AUTHOR
Prof. dr. Paul Timmers

POSITION
Research Associate

ORGANIZATION
University of Oxford

Advancing accountable cybersecurity as a global common good, to alleviate security and sovereignty concerns

In this article I will argue in favor of advancing accountable cybersecurity as global common good to contribute, even if limited, to alleviating both cybersecurity and sovereignty concerns.

Over recent years we have seen countries getting increasingly anxious about their sovereignty. They feel the triple threat of increasing international tensions, disruptive digital transformation throughout economy and society, and an explosive growth of cyber-attacks and cyber-incidents. A 'sovereignty gap' is opening up, as Oxford University Professor Kello calls it.

Leaders from across the political spectrum are worried whether they have the means to overcome this gap or whether it will get even worse due to having dropped the ball on their national strategic autonomy.

Strategic autonomy is a notion that in the past was mostly used by France from a military and defense perspective and by India from the perspective being an independent state relative to Beijing, Moscow and Washington. But nowadays strategic autonomy is much wider. It is the ability to decide and act upon key features of the future of your economy, society and democracy. You could say, strategic autonomy is a means to realize sovereignty.

But then, how do you achieve strategic autonomy? Which knowledge and technologies and other capabilities should a country master? Which research, manufacturing, and deployment capacities do you absolutely need? What are the assets to keep in your own hand as a country?

Perhaps the USA and China are resourceful enough to build the necessary strategic autonomy on their own. For other countries there are three approaches they can follow. I will address them here from the perspective of cybersecurity and the related accountability.

The first approach to strategic autonomy in cybersecurity is risk management. This means trying to detect and counter threats as much as possible, to harden as much as possible critical infrastructures like electricity, transport or health or electoral systems as these also get hacked nowadays.

Risk management is not perfect, it is a best-effort and likely leaves a residual risk. Accountability means demonstrating that indeed the very 'best' has been done. This can be a requirement by law, such as in the EU by the Network and Information Security Directive. It can also be market-driven, coming from cyber-insurers.

The residual risk can imply to accept that lives may be lost, as may have happened during the Wannacry cyber-incident. Or perhaps a kill switch remains hidden in a critical infrastructure. Or intellectual property gets siphoned away to the extent that in the longer-run the economy gets fatally weakened. Who is accountable? This must have a political answer. No wonder that countries try to counter these risks by engaging politically and seeking to agree on global norms and values such as 'do not harm civilian infrastructure' and information sharing on incidents.

The second approach is to limit collaboration to likeminded partners. This is the strategic partnership approach. Buying and selling, sharing knowledge, etc. then only happens with trusted states and companies. Accountability is within the partnership and linked to hard law or softer mutual

→ AUTHOR
Prof. dr. Paul Timmers

agreements. For example, it could be a bilateral agreement implementing a third-country clause of national or regional law on data protection or cybersecurity certification. This is complemented by adequacy in terms of trust in each other's political and judicial systems.

Strategic partnerships do not sit easy with global business. Companies do not like to be labelled as likeminded or not likeminded. And even between countries, today's friends in cybersecurity can turn into tomorrow's opponents in other but related matters such as trade. Strategic partnerships may also suffer from lack of resources. Strategic cybersecurity expertise and assets can be costly, even more so with a narrower supplier base, think of 5G security.

Is there a way to escape to some extent the downsides of risk management and strategic partnerships? There is a third approach. This is to promote cybersecurity assets as a global common good. What does this mean? Think back of the days when the internet was presented as an asset for all of humanity. Its creators wanted it to be technologically open. Its governance had to be by a widely distribution set of stakeholders, without a single government being able exercise sovereign control.

Obviously, this ideal did not get realized, in fact far from it. Still, the idea of a global common good is not dead. For example, several countries are today promoting a secure public core of the internet, the domain name system, as a global common good. Can we imagine that we declare the security of other parts of critical digital infrastructures as a global common good? For example, the control systems of utilities or of global logistics? Is it feasible to pursue global common good in cybersecurity? At least as a third way complementary to risk management and strategic partnerships?

Without being naïve, I can see some perspectives. Firstly, technology can help. Such as open source and distributed security control with blockchain. Secondly, a global common good approach also requires global governance and accountability. This must come from partnerships of states, industry, and civil society. Though far from perfect there is some governance we can build on. Think of the UN, ICANN, IETF, the World Wide Web Consortium, global industry alliances such as oneM2M for standardization of the Internet of Things, and efforts such as The Hague Charter for Accountability in the Digital Age.

As an aside, a global common good approach enables states to focus their limited resources on their internal and external legitimacy. It may therefore strengthen rather than weaken their sovereignty!

We can also learn from the past. In the 1980s a dramatic global challenge was identified: the growing hole in the ozone layer. In response, scientists, policymakers and industry joined forces to reduce the emission of CFCs, the damaging chemicals. Within two years, the Montreal Protocol was signed, CFCs were banned and — though it lasted many years — the ozone layer has started to recover. It was a major success in protecting a global common good. Why did it work? Perhaps because the precautionary principle to prevent future global catastrophic damage was accepted. And because a degree of accountability, even if not perfect, could be put in place.

We may learn from this to advance an accountable global common good approach in cybersecurity.

AUTHOR
Prof. Dr. Jaap van den Herik

POSITION
Professor

ORGANIZATION
Leiden University Centre of Data Science

The Future of Accountability

Are we happy with the current way of storing data? A typical answer is: Yes, technologically we are satisfied with the available means; No, managerially we are not so pleased since we worry about our privacy. This column is meant to warn you that privacy is not the main issue; the delicate one is the storage itself and only thereafter comes privacy. Two observations and one speculation will lead you to a new situation.

Observation 1: At this moment (2020) the amount of data is rapidly increasing worldwide with a compounding annual growth rate of more than 60 percent.
Observation 2: There is a clear shift of importance from storing data towards storing metadata.
Speculation: Within two years it is expected that the partition of metadata and data will be 80% (metadata) and 20% (data).

Several forecasters predict that around 2025 there will be a request for 175 ZB data storage (ZB means Zettabytes; 1 ZB is 10 to the power 21 bytes).The important accountability question is: *What is our future in this respect?*

It is well known that Deoxyribonucleic acid (in plain words: DNA) stores our genetic information. It does so quite effectively. The prevailing challenge reads: Is it possible to store non-genetic information (say plain (meta)-data) in DNA boxes? How much can we store in the DNA convex hull of our little finger? Quite a lot. Therefore, it may be sufficient to communicate that all current data and metadata (33 ZB) can be stored in one big hall. This sounds promising, but the way to it is full of obstacles. Two of them are: (a) prohibitive costs and (b) slow access times. The attempts to realise these ideas are currently in their infancy, whereas the deadline is only five years away. Hence, in the next three years researchers of the highest calibre should perform investigations into this direction. The change is comparable with the transition from coal and oil to electricity. The world is ours, we are accountable for the decisions to be taken .For the digital world, a possible transition towards DNA storage is of utmost importance. It is not clear whether slow access is in favour of privacy or even detrimental. In summary, we have to prioritise our research agenda from the point of view of data with respect to the internet of things.

Acknowledgement
The author is happy to acknowledge the International Data Corporation (IDC) for their publications (e.g., by Andy Patrizio) and for his collegial talk with Professor Barend Mons (Leiden University) as sources of inspiration.

AUTHOR
Oleg Volkosh

POSITION
President

ORGANIZATION
Mediaplus Group Russia

The main event of the 21st century in the field of media and marketing was the emergence of social networks. For the first time, we were able to cover, analyze and communicate with more than 3.5 billion people worldwide. This is by far the largest and most interactive channel of communication between people on the planet. The main aspect of my report is how working with social networks, marketing technologies and artificial intelligence can and should save lives. We must understand that with all the outward positivity and glamor of some of the content on social networks, there is a lot of pain, human tragedies and statements about suicidal tendencies or preparedness.

After conducting an analysis of such content only in Russia and only during the summer month of July 2019, we identified about 10,000 posts of people with a statement of readiness to die. This is scary statistics, despite the fact that according to various sources, around 18,000 suicides per year occur in Russia. Many of the people who committed suicide left a mark on the social networks, and many of them fell under the negative effect of such content, which is now absolutely uncontrollably spread within social networks. At the same time, different countries are trying in their own way to solve this painful problem, but for some reason, by means of the 20th century, not the 21st century of technology, financing, for example, call centers for which no one from the young generation has been contacting for a long time. At the same time, all the capabilities of social networks, machine learning and artificial intelligence, are not used.

My main message is that we can and must save the lives of hundreds of thousands of people in the world using interactive social networks, artificial intelligence, data analytics and ensure effective communication using all modern technologies while being aware of what is happening every minute in the posts of millions of people and dialogue with those of them who are already about to cross the last line. All the capabilities and technologies already exist for this. It remains to find socially responsible institutions and start a global project on how to save millions of lives.

AUTHOR
Cédric Wachholz, Prateek Sibal, Melissa Tay Ru Jein, Rachel Pollack

ORGANIZATION
UNESCO

Trust, it is argued, facilitates 'interactions between human agents, artificial agents or a combination of both'. A characteristic feature of trust is 'delegation without supervision'. For instance, daily interactions such as asking a friend to pick up a child from school or requesting a colleague to represent one at a meeting are enabled by trust.

The digital sphere is no different; interactions mediated by technological tools require trust to allow users to engage with them effortlessly and without concern over potential violation of human rights and dignity. However, trust in technologies like artificial intelligence (AI) have been eroded by concerns over bias and discrimination, violations of privacy, and loss of human agency.

There are numerous examples of decisions reached by algorithms that reflect societal biases. UNESCO's report *Steering AI and Advanced ICTs for Knowledge Societies* highlights several cases of racial and gender bias in AI systems, including the following:

- Major facial recognition software on gender identification showed higher error rates for darker-skinned female faces (35%) compared to lighter-skinned male faces (1%), likely because the data used to train algorithms are 'overwhelmingly composed of lighter skinned subjects.
- Language translation engines propagated gender stereotypes by identifying some professions as 'male' and others as 'female'.
- Recruiting software was found to downgrade resumes that contained the word 'women' because it had been trained on men's resumes.

These examples illustrate the need for accountability, fairness, explainability and transparency in the way that technologies liked AI are developed and used. Often seen as a 'black boxes', the complexity of AI systems makes them hard to understand by humans. In this context, the UNESCO report points out the need to 'develop norms and policies for improving openness, transparency and accountability in automated decisions taken by AI systems through methods such as ex-ante information disclosure and ex-post monitoring of automated decision-making.'

Such norms and policies on ethical principles contribute to curtailing concerns over fairness and infringement of human rights. While many governments have recently developed strategies on AI, regional disparities remain. A 2019 study reports that out of 84 documents containing ethical principles or guidelines for AI, there were no African or South American at national level. In contrast, there were 20 such documents in the United States and 19 in Europe. To date, there is no normative instrument on the ethics of AI that exists at the international level.

To fill this need, UNESCO is developing a standard setting instrument on the ethics of AI. Based on multistakeholder consultations and intergovernmental deliberations between our 193 Member States, the recommendation will have been developed by a multidisciplinary expert group representing all regions and undergone inclusive and open consultations, reflecting the world's cultural diversity, while anchoring the future in universal human rights and human dignity.

I would like to conclude with a quote from the French writer Molière: "accountability is not only what we do, but also what we do not do, for which we are accountable".

If we are to ensure trust in our digital future, we must act now.

The 2019 Summit is made possible with the financial contributions of:

Click on the logo to go to the organisation's website

Summit Sponsors

The Hague

UNESCO

Microsoft

THALES

Deloitte.

International Media Sponsor

BARRON'S

Local Media Sponsor

DIPLOMAT TV

iBestuur

The content of the 2018 and 2019 Summit is made possible through the continued support of representatives of the following organizations.

Click on the logo to go to the organisation's website

Colophon

The Institute for Accountability in the Digital Age would like to thank the audience, speakers, panelists, moderators and other volunteers who have contributed to the Summit and its success. Especially to Sara Kemppainen for her outstanding support.

Institute for Accountability in the Digital Age
Frits Bussemaker, Chair
Arthur van der Wees, main author of the report
Michel Rademaker, board member

Design: Stephan Csikós, The Hague

Institute for Accountability
in the Digital Age (I4ADA)

Postal address I4ADA
Lange Voorhout 1
2514 EA The Hague
The Netherlands

+31 (0)70 318 48 40

contact@i4ada.org
www.i4ada.org

INSTITUTE FOR
ACCOUNTABILITY
IN THE DIGITAL AGE

www.I4ADA.org