

LEGAL **BUSINESS** WORLD

• Legal Business World Publications • 2020 • www.legalbusinessworld.com

World Legal Summit Special Edition

Regional Summaries, Summit Themes, Jurisdictional Frameworks, Topics on Technology Governance, and more ...

Contributors: Aileen Schultz, Cara Sabatini, Alice Namuli & Collins Tumukunde, Federico Gabbricci & Deborah Bolco, David N. Alfred & Josh Lee Kok Thong, Paula Figueiredo, Mark Potkewitz & Ryan Carrier, Tatiana Revoredo, Myron Mallia-Dare, Daniel Araya, Alice Nawfal

World Legal Summit

WLS

WORLD LEGAL SUMMIT

Introduction

Dear friends of sustainable technology,

This special edition e-zine is meant to give you a lens into the concepts and vision driving the World Legal Summit (WLS). Most importantly, it is an open invitation to get involved. The WLS was launched in 2019 as an experiment in technology governance aimed at bringing technical and legal communities together to bridge the siloed discussions currently existing amongst these communities. Worldwide we have technologists inventing and improving new technologies that are reimagining our globally collaborative future. This future could and should be a very beautiful one for us all. However, in order for us to arrive at this beautiful future, these communities need to come together with their shared domains of expertise. There must be worldwide collaboration in promoting the sustainable evolution of these technologies and the new global systems they're making possible.

While legal and governance communities are emerging to solve some of these issues in different parts of the world, these groups are often focused on one or just a handful of jurisdictions. And more often than not, the voice of the technologist is missing

from these conversations. The World Legal Summit is focused on our global jurisdiction and is designed to bring legal and technology communities together in collaboration on these topics. The WLS is a community driven platform. It is designed for the discussion and application of the legal frameworks governing new technologies, as well as to provide an environment where technologists can learn about and develop legal insights into the technologies they're developing.

It is our belief that a collective of insights from all corners of the globe distilled into a common understanding, is far superior than the predominantly centralized frameworks currently in place. The World Legal Summit intends to promote this collective, and over time to uncover a common dialogue that is representative of a community of truly global minded citizens with the best interest of all at heart.

We invite you to read on and learn more, and hope that you will join us in the co-development of a globally sustainable future.

Yours in legal transformation,
The WLS Team

World Legal Summit

Latest Blogs

Safety and Security in AI Systems (<https://worldlegalsummit.org/safety-and-security-in-ai-systems/>)

Borderless Internet, What's Law Got to do With it? (<https://worldlegalsummit.org/borderless-internet-whats-law-got-to-do-with-it-part-1/>)

Basic Principles Guiding AI Frameworks Around the World (<https://worldlegalsummit.org/basic-principles-guiding-ai-frameworks-around-the-world-part-i/>)

Follow WLS on Twitter (click on the feed)



Management/Publisher

LegalBusinessWorld Publications
Joek Peters | CEO | President
Allard Winterink COO | SVP

jpeters@legalbusinessworld.com
awinterink@legalbusinessworld.com
© LegalBusinessWorld™

Editorial

LegalBusinessWorld Publications
Editorial Dept.
MBL Media

Sales Representatives International

Michael Blakely (US/Canada)
mblakely@mblakelysalesandmktg.com

Telesales: Fox Associates
800-440-0231 ext 116
Adinfo.lbw@foxrep.com
Or contact our media department at
info@legalbusinessworld.com

Design & Layout

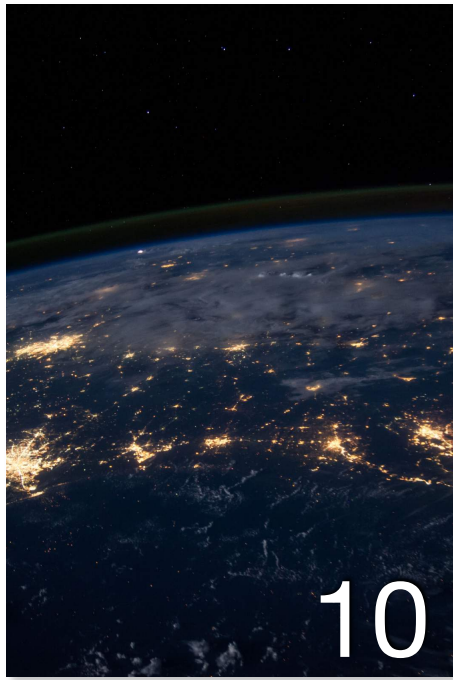
LateNight studio's
info@legalbusinessworld.com

This Special Edition is published by Legal Business World Publications. Legal Business World is partner of World Legal Summit.

WLS

WORLD LEGAL SUMMIT

Getting involved & inquiries
contact:
info@worldlegalsummit.org



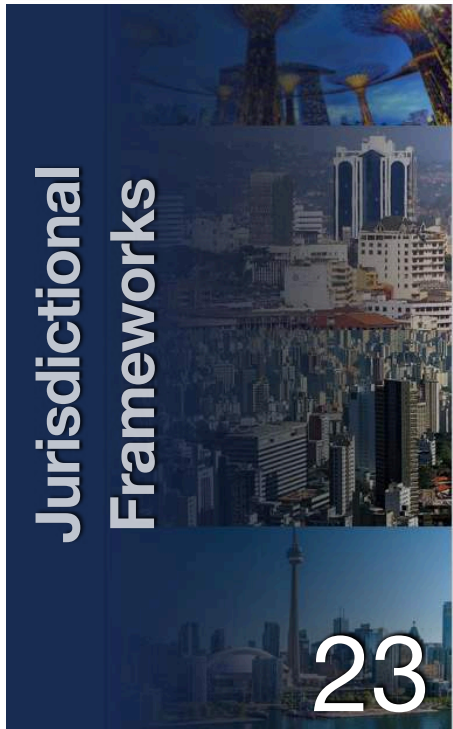
10

The Inaugural Year
Sets the Stage

14



17



Jurisdictional
Frameworks

23



24



36

Introduction, WLS Team

3

World Legal Summit Overview

Informed Technology Development for a Globally Sustainable Future, Aileen Schultz

10

The Inaugural Year Sets the Stage, WLS Team

14

WLS Global Impact Award: ValiData, A Solution that Demands Sustainable Identity Systems, Cara Sabatini

17

World Legal Summit : Regional Summaries

Section overview Jurisdictional Frameworks, WLS Team

23

Legislative Environment in Africa: Data, Digital Identities, Blockchain and AI, Alice Namuli & Collins Tumukunde

24

Regulatory Developments in AI, Decentralised Technologies, Data Protection and Cybersecurity in the Asia-Pacific, David N. Alfred & Josh Lee Kok Thong

36



<u>European Summary, Federico Gabbricci & Deborah Bolco</u>	48
<u>Short Overview Latin America, WLS Team</u>	56
<u>Brazilian Legal Framework in Connection with the World Legal Summit, Paula Figueiredo</u>	60
<u>North America, Aileen Schultz</u>	64
World Legal Summit : Technology Themes	
<u>Section overview Topics on Technology Governance, WLS Team</u>	77



<u>Renewing Multilateral Governance in the Age of AI, Daniel Araya</u>	78
<u>Product Liability and AI: Whose Really at Fault?, Myron Mallia-Dare</u>	82
<u>Tech Governance: The future of Digital Identity, Alice Nawfal</u>	86
<u>Self-Sovereign Digital Identity: The Management of Identities and the Ability to Prove Who We Are, Tatiana Revoredo</u>	92
<u>Suggested legislative measures to overcome the contact tracing “trust gap”, Mark Potkewitz & Ryan Carrier</u>	102
<u>ForHumanty A Proposed Framework for the Auditing of AI Systems</u>	110



World Legal Summit

Overview







Informed Technology Development for a Globally Sustainable Future

By Aileen Schultz, Founder & President, World Legal Summit; Senior Manager, Labs Programs at Thomson Reuters

The world is rapidly transforming with the development and increasing adoption of new technologies. New technologies are affecting existing systems, and creating the path toward future global systems that were previously unimaginable; for example, a universal currency, self sovereign identities, or truly decentralized governance. Right now these technological developments are happening in silos,

and emergent global systems remain underdeveloped and ill informed.

The core mission of the World Legal Summit is to bring legal and technology communities together in an open dialogue addressing issues at the intersection of technology and needed governance models.

On the one end we have law making groups consisting of professionals across legal, policy, government, and academia. These groups are driving toward the development of new legislative frameworks for managing these emerging technologies. These efforts are intended to maintain and promote the integrity of new era legal frameworks, and are meant to fill gaps in governance for new technologies. These efforts are imperative to ensuring the social contracts underpinning legal systems continue to grow and improve, and that they don't falter under the speed of technological transformation.

On the other side of the equation, we have software engineers, venture capitalists, data scientists, entrepreneurs, and generalized technology passionate driving toward the previously unimaginable with the development and adoption of new technologies. New technologies and their applications are increasingly solving some of the world's most pressing challenges, as well as opening up whole realms of new possibilities across every sector imaginable. At this rate, we certainly don't want to slow things down unnecessarily. As such, it is equally fundamental that we include the technologists voice in the legislative transformation affecting these technologies. We need to do

everything in our power to sensibly regulate while not succumbing to bureaucratic nonsense that would unnecessarily impede this impressive rate of technological innovation.

The World Legal Summit intends to bring both sides of the equation together in a collaborative dialogue that does not neglect each side's core drivers; encouraging our sensible coexistence, while also promoting the rapid innovation of new technologies. It is our belief that these technologies are painting a future of global collaboration like never before, inclusive of systems that will support the development and application of universal human rights, global economies not dependent on political whims, and the possibility of a truly global citizenry not dependent on government for their social inclusion.

Our “Technology Pillars”, Technology Shaping Global Systems

While there is a consistently growing body of new technologies affecting our global systems, we believe there are three core technology categories that are facilitating the possibility and growth of these systems. We have established these categories as our “WLS Technology Pillars”, as follows:

Identity & Decentralized Technologies	AI & Autonomous Systems	Personal Data Governance
<p>Inclusive of digital identities and surrounding technologies (e.g. biometric authentication), as well as decentralized technologies like blockchain and their solutions for identity management. Collectively, these technologies are making possible decentralized identity frameworks independent of intermediaries.</p>	<p>Inclusive of artificial intelligence technologies and their ethical application, as well as the autonomous systems they're making possible, such as the mass use of smart contracts, or "self executing algorithms". These technologies have the ability to curate and support efficiencies in decentralized systems and their governance.</p>	<p>Inclusive of the complete system of personal data surrounding nearly every person on this planet, both digitally and physically through credentials, health records, employment contracts and endless others. This data is accumulating in governments, companies, and institutions, and needs better governance to protect individual rights.</p>

These technology pillars are not exclusive of each other, but rather they intersect with collective dependencies and capabilities. Let's now review how these categories are critical to emergent global systems, and how they intersect with each other. We will start with 'Identity and Decentralized Technologies'. If we think about the core of how law functions, it is the social contract. Core to the social contract are people that make up the collective society. The collective society is in turn made up of the individual, and the individual only exists in a legal context in so far as they can be identified as a person in that system. However, current identity infrastructures are broken, and we're moving toward a more globally connected world in need of new systems. There is a growing indication that we are moving into a possible future framework that operates independent of, or in conjunction with, federalized dependencies. We need only look at the budding possibility of a universal currency or "[supercurrency](#)" to illustrate just how imminent this possibility is. Core to the sustainability of this framework is a sound and decentralized identity infrastructure.

Now let's take a look at where 'AI and Autonomous Systems' have a role. Let's imagine a world in which this global governance model begins to become a vivid reality. Then what? How does such global governance ensure its integrity? How does it operate as a sum of legal inputs from multiple jurisdictions? While there is a long way to go before artificially intelligent systems are unbiased and ethically sound, these systems are offering the possibility of self-executing or human-independent government and justice models. In addition, these technologies are creating efficiencies that enable scaled systems like never before. Likely a terrifying consideration for most. However, for those who

have been subject to human led government corruption or poorly executed judicial systems, it is a very different story and these people are likely to see the optimism in these possibilities.

Finally, let's consider how data is the foundation of those first two technology pillars. How is it that we've come this far with technological developments in such a short period of time? Data. The sheer volumes of data now accessible about people and social systems is phenomenal and almost incomprehensible. Our abilities to work with and analyze this data are increasing ten fold, for example, we already have out of the box machine learning models to process various sets of unstructured data. Big data is titled the "new oil" very rightly so, and not just because of its value, but because it is driving the engine of emerging technologies and the future global systems they're making possible. It is not news that legal models for regulating the use of this data and the protection of the persons it belongs to are desperately needed.

With these considerations it becomes clear how these three technology pillars intersect and collectively are at the core of emerging global systems. It is this understanding by which the World Legal Summit intends to operate, with the purpose of promoting needed dialogue around these emerging systems and promoting their sustainable development..

About the Author:

[Aileen Schultz](#) is a Toronto based award winning innovation strategist with a global footprint, and a passion for creating better systems for exponential change. She is particularly focused on effecting change at the cross sector between law and technology.

The Inaugural Year Sets the Stage

The first year of the World Legal Summit was a grand experiment. It proved the hypothesis that technology and legal communities could come together cross-jurisdictionally and collaborate in the formation of legal insights, as well as the application of these insights to the sustainable development of new technologies. It took place across all major world regions, including locations in [30+ cities across 20+ countries](#). The inaugural WLS initiative brought together organizations across academia, non-profit, legal, government, and technology. It built a global community of over one thousand experts and enthusiasts across those domains. This community was focused on discussing issues of governance within our three core technology categories: identity and decentralized technologies, AI and autonomous systems, and data governance.

Each host location participated in the formation of insights around key categories of technology legislation and policy in their regions, which is being summarized for digital publication in late 2020. These host locations were each focused on answering critical questions about the legislative frameworks, or lack thereof, for these technology pillars. In addition, hosts and participants discussed what is required to make these legal insights accessible to technologists. In order to accomplish these aims, the first year of the WLS happened in two parts. These were separate events that each happened simultaneously across participating jurisdictions. Step one focused on the research and understanding of these concepts, to be followed by the second step which was focused on the development of those insights into the actual technologies.



Part One - Informing, Aug 1st 2019:

Designed to facilitate the understanding and formulation of global insights about legislative and regulatory frameworks dealing with the WLS Technology Pillars and their related global systems.

Part Two - Action, Sept 6-8 2019:

A world wide development sprint, designed to bring the insights and understandings from part one together with individuals and organizations world wide. It created an environment in which individuals and organizations working on the development of these technologies could discover ways to develop legal insights into these technologies; in such a way that supports these technologies' role in developing our globally sustainable future.

The complete insights and highlights of the 2019 inaugural year will be released digitally later this year. Interested to know when it's launched? Sign up for updates at www.-worldlegalsummit.org

What's next for the World Legal Summit?

The inaugural year of the WLS proved the

framework for cross jurisdictional collaboration in driving progress for technology governance. In particular, it proved the passion that many experts have in applying this framework to those three technology pillars.

There were of course many lessons learned. These learnings have been applied to future iterations of the WLS initiative and how we intend to grow as an organization.

While the official WLS events are the core initiatives driving the organization, there is opportunity for the community to do much more. Primarily, there is opportunity here to continue developing research as well as POCs in these core domains, and to further develop the expert community involved in contributing their perspectives.

We very much operate by the belief that there is great perspective to be had from the social collective, and the insights that emerge by way of distilling global trends. The more diverse this community becomes by way of involved jurisdictions and the ecosystem, the more impactful these insights will be.

The second edition of the WLS events are planned to take place in Autumn of 2021, on a biennial model. If you or your organization would like to learn more about hosting a location, sponsoring or otherwise getting involved, please contact us at info@worldlegalsummit.org

WLS Global Impact Award: ValiData, A Solution that Demands Sustainable Identity Systems

By Cara Sabatini, Researcher & Writer, World Legal Summit

The race to stop the spread of the new coronavirus has generated numerous technological solutions, from contact tracking technology to biometric digital ID, while raising questions over the sustainability and integrity of the solutions in the long-run.

In a pandemic-stricken world where access to healthcare is primarily based on [nationality](#), being able to prove one's identity is critical. Those without proof of ID, such as stateless refugees, risk being barred from accessing everything from relief funds to healthcare services. Legal Project Management, the Legal-World-Cafe, as well as the matchmaking tool EvPitch.



Further, once a vaccine is developed, it will be important to ensure that each vaccine reaches a real individual, explained Prashant Yadav, a senior fellow at the U.S.-based Center for Global Development, to Canada's [Globe and Mail](#). "Corruption, leakage, and even accidental duplication waste precious supply and are deadly", Yadav told the Globe.

The distribution of vaccinations could pose problems not only for individuals who are unable to prove their identity, but also for the governments and healthcare systems tasked with administering a potentially limited supply of vaccines.

Though the new coronavirus may compound barriers associated with lack of verifiable identification, the issue of “invisible people” is not new, and presents myriad problems for both individuals and societies, particularly in the case of refugees.

According to the [World Bank](#), more than one billion people around the world are unable to prove their identity, meaning they are barred from accessing vital services such as health-care, finance, education, and social programs.

Large-scale lack of identification is what inspired the Internet Bar Organization (IBO) to launch the “Invisibles Project,” which aims to provide secure identification to people lacking proof of ID and to promote best practices for digital identity.

Digital Identity Around the World

More than 30 countries have employed some form of digital identity as a means to verify legal status or provide government services in a more efficient and expedient manner. While the coronavirus pandemic has meant delays or setbacks for some digital ID programs, it has also elevated interest in such systems.

In March, the US [pushed back](#) the enforcement deadline by a year for their Real ID drivers’ licences, as government agencies across the country closed their doors to the public. On the other hand, Lichtenstein recently rolled out a [pilot program](#) to equip citizens with biometric bracelets that collect data on vital metrics, including temperature and breathing rates, to track potential new coronavirus cases. Of course, not everyone will jump at the chance to wear a bracelet that monitors their breathing rates, as they consider the im-

plications such a program could have for their privacy and data security.

Digital ID solutions are certainly not without their challenges or controversy, particularly when they clash with existing legal frameworks. The Supreme Court of India has issued several rulings on the country’s biometric-based identity system, Aadhaar, that affirm the constitutionality of the system but also affirm privacy rights and access to education and financial institutions even for those not registered in the system. Throughout its lifetime, Aadhaar has faced criticism for its possible [data breaches](#) and vulnerability to [exploitation](#) by third parties. A 2018 supreme court [ruling](#) set limits on how the data is used, restricting the use of Aadhaar to government services as opposed to its private-sector purposes like opening bank accounts and obtaining SIM cards. While the court rulings do not solve all of Aadhaar’s issues, they do point to the need to have comprehensive legal frameworks that protect the rights of citizens in order to ensure the sustainability of a digital identification system.

This speaks in part to the goals of the World Legal Summit, which hosted its inaugural event in 2019 to bring together technologists, ethicists, and regulatory experts to generate insights and foster sustainable solutions for the development and use of technology around the world.

ValiData, A Solution for Decentralized Identity Management

The IBO sought to build out aspects of the Invisibles Project by teaming up with the Houston-based coding school Digital Crafts at the 2019 World Legal Summit.

During the inaugural WLS development sprint aimed at developing legal insights into technologies Houston's "Team Validata" stood out for its work on the Invisibles Project, and was granted the first WLS Global Impact Award for its potential to address an area of significant social concern on a global scale.

"The Global Impact Award is intended to recognize projects that use emerging technologies to support the development of sustainable global systems. The work that the IBO does, including project ValiData, addresses problem areas in great need of more development world wide." Aileen Schultz, President, World Legal Summit

The Invisibles Project seeks to provide identification to stateless refugees and others lacking ID with a form of blockchain-based identification so that they can access opportunities otherwise unavailable to them - ranging from health and education to career opportunities and access to justice.

Digital ID has long been proposed to improve state capacity to deliver essential services, particularly in the developing world where birth registrations may be lower and government infrastructure may be lacking or struggling to reach populations in rural areas.

Data from the [World Bank](#) show that only 20% of births were registered in Bangladesh in 2014 and only 11% in Zambia in 2018. Ethiopia and Somalia show some of the lowest birth registration rates. A 2013 [study](#), published in the Bulletin of the World Health Organization, showed that children in Ghana who received a polio vaccine were more likely to be registered at birth.

Beyond access to healthcare and education, lack of identification also restricts mobility. Many people fleeing the crisis in Venezuela [lack documentation](#) or visas typically required to enter neighbouring countries, and many struggle to find work once they reach their destination. The UNHCR [states](#) that hundreds of thousands of Venezuelans without documentation or legal status to remain in nearby countries lack access to basic rights, such as education and the ability to work, which leaves them vulnerable to exploitation.

The ValiData solution emerged from "The Invisibles Project", a project that evolved from other IBO initiatives that seek to promote access to these basic forms of justice. But access to justice is more than providing people with access to a national legal system, explained IBO president Jeffrey Aresty. It's also about providing individuals access to education and employment by ensuring that they have ways to prove their identity and credentials.

The IBO has worked on numerous projects to promote access to educational and income opportunities around the world. In 2018, IBO [partnered](#) with ODEM to make higher-education "more accessible and affordable" on a global scale. Their pilot program aimed to create a means for students, educators, and institutions to share information and interact through smart contracts. Another IBO initiative includes [PeaceTones](#) which helps musicians to protect and market their music by providing them information on their legal rights and marketing techniques.

At the Houston location of the World Legal Summit, the IBO asked participants to build

out a framework for validating the type of data that the Invisibles Project needs to carry out its solutions.

Specifically, participants set out to create a system to collect and store data that could be used to issue blockchain-based identification to healthcare workers in Bangladesh, some of whom may be in rural areas, volunteers from overseas, or individuals displaced from conflict zones like Myanmar and do not have access to their professional identification or credentials.

The Validata team incorporated an encrypted database using NoSQL as part of their plan to provide verifiable credentials to healthcare workers in the South Asian country.

Newly minted software engineer Robert McCutchen worked on the Invisibles Project as part of Team Validata, along with teammates Umreen Imam, Taliaa Tauatolo, and Philip Kennedy. At the time, McCutchen was completing a coding bootcamp at Digital Crafts.

“We learned a lot not just about the situation with refugees but also with issues related to information security,” said McCutchen about working on the Invisibles Project with his team.

McCutchen explained that using an encrypted database would allow them to retain some administrative control over the program.

“You need to rely on legacy to some degree,” said Aresty about the solution. He explained that while the pertinent information would eventually be stored on a blockchain as a way

to ensure security, it was also important not to overload the ledger with unnecessary data.

“The blockchain piece that we’re using is just the last step,” said Aresty.

McCutchen was grateful for the learning experience he had at the WLS. “There were a lot of legal implications that we were ill prepared to handle,” said McCutchen about the challenges his team faced while building out the solution. He cited the European Union’s General Data Protection Act and California Consumer Privacy Act that place stronger protections on user data.

Both the European and Californian legislation establish definitions for biometric data. However, the GDPR goes further than the CCPA in that it classifies biometric data in a separate category subject to more protection. Though there are exceptions, under the GDPR, such data cannot be processed without consent.

As biometric data becomes more prevalent in countries around the world, so do the concerns raised by privacy advocates, scientists, and policymakers over its use. While digital rights advocate Brett Solomon acknowledges that digital ID can mean financial security and opportunity to refugees around the world, but also warns against the perils of mandatory digital ID systems. “In the design and deployment of Digital ID systems, we must advocate for the principles of data minimization, decentralization, consent, and limited access that reinforce our fundamental rights,” writes Solomon in [Wired](#).

Cybersecurity expert Jayshree Pandya cites concern over the statistical nature of biometric

identification and its possible incapability with current legal systems. Pandya writes in [Forbes](#), “from a legal perspective, anything less than 100% probability of a match may or may not be considered acceptable for identity authentication.” Though Pandya believes the performance advantages of biometrics currently outweigh the security and privacy risks, she stresses the need for interoperability and global standards to address the complex challenges precipitated by biometrics-based applications.

Indeed, a key part of the WLS mission is to support collaboration between legal and technology communities toward the development of frameworks for technology governance.

McCutchen’s take-away from working on the project as part of the WLS was learning “how interconnected law has become with technology and how legal systems have been incorporating technology to improve justice systems around the world.”

Since the 2019 WLS, the IBO has worked on other digital credential-based solutions to promote professional access, including a recent project that brings together high school students in Texas and Zambia to take an online cinematography course together, where students have the opportunity to gain credits while also learning from each other.

In a world where our interactions and institutions are increasingly virtual - accelerated by current social distancing rules brought on by the coronavirus pandemic - the need for trustworthy forms of interaction is perhaps

more salient than ever.

Aresty, a long-time proponent of the need for secure legal identities to promote access to opportunity and prevent fraud, believes trustworthy identity has a key role to play in building out our current systems and mitigating what he calls a “trust deficit” in society.

“Ultimately, identity is the key thing that is going to determine whether you have a system you can trust or not,” said Aresty. “We need a system of identity that works again.”

About the Author

Cara Sabatini is a researcher and journalist in Toronto, ON. She holds a BA in Ethics, Society & Law from the University of Toronto and certificates from the University of King’s College and York University. Her areas of interest include emerging legal concepts, access to justice, and so called soft law.





World Legal Summit

Regional Summaries



Section overview

Jurisdictional Frameworks

The WLS seeks to explore global patterns in legislative transformation for emerging technologies. We do this by reviewing insights from all world regions, and conducting further research on transformations at the jurisdictional level. Further to this mandate, the WLS is focused on fostering a robust and diverse global community of experts and enthusiasts across the legal and technology domains.

While the WLS was successful in its inaugural year in building this research and this community across all continents (except Antarctica), some regions have so far been underrepresented; such as the Middle East and parts of Asia. As the WLS moves beyond its inaugural year, it seeks to grow to be inclusive of perspectives from all regions world-wide, and openly invites all to get involved.

The following series of articles are written by members of the WLS community and

survey the current legislative landscape governing our core technology pillars in their respective jurisdictions. We have found that the best organization of regions participating in the WLS are as follows, and have organized this section in this format: Africa, Asia-Pacific, Europe, Latin America, and North America.

These articles are a ‘sneak-peak’ into the insights that will be shared through the digital publication, to be released later this year (2020). This digital publication will be made available on the WLS website (www.worldlegalsummit.org), and will detail laws world-wide for all WLS 2019 participating locations, as well as perspectives shared during this inaugural summit.

Interested?

If you or your organization are interested in getting involved in your region, you can share your interest with us at info@worldlegalsummit.org



Legislative Environment in Africa: Data, Digital Identities, Blockchain and AI

By Alice Namuli, Partner and Head of Technology and Innovation at Katende, Ssempebwa & Company Advocates and Collins Tumukunde, writer for the Legal Innovation Hub in Uganda with a background policy research

OVERVIEW OF DATA PROTECTION LAWS IN AFRICA

Data Protection has been gaining ground in Africa. Today, out of 54 countries, **25** have passed data protection laws, the latest countries being Uganda, Nigeria and Kenya. Other

countries have introduced data protection bills which are under discussion or waiting to be on the legislative agenda.

On a regional level, some measures have been taken to encourage and support the enactment of data protection laws:

In 2010, the Economic Community of West African States (**ECOWAS**) adopted a Supplementary Act on Personal Data Protection. A year later, a Supplementary Act on Cybercrime was enacted. So far, two thirds of the ECOWAS member states have passed data protection laws, except Togo, the Gambia, Guinea Bissau, Sierra Leone and Liberia.

In 2013, the Southern African Development Community (**SADC**) published a Model Data Protection Act. Since then, only two countries have enacted data protection laws. Counting the five SADC member states which already had privacy laws in place, seven out of 16 member states have a data protection legal framework today.

In 2014, the African Union adopted the Convention on Cyber Security and Personal Data Protection (the **Malabo** Convention). It is a comprehensive document covering electronic transactions, privacy and cybersecurity. To date, the Malabo Convention has been signed by 14 states and ratified by five countries out of 55 member states (Western Sahara being part of the African Union).

Kenya

The Data Protection Bill, 2019 was signed into law ('the Act') by President Uhuru Kenyatta , on 8 November 2019, establishing requirements for the protection of personal data. The Act's objectives and scope are to regulate the processing of personal data and to ensure that the processing of personal data is guided by the legislated data protection principles. Other objectives are to protect the privacy of individuals and to establish the legal and institu-

tional mechanism to protect personal data by providing data subjects with rights and remedies.

The primary overarching principle being that personal data should only be collected directly from the data subject and used (be it for processing, commercial use or otherwise) with the **express consent** of the subject. Where personal data has been accessed or acquired without authorization and there is a real risk of harm, a data controller is required to notify the Commissioner without delay, within seventy-two hours of becoming aware of such breach, requiring that person to take such steps and within such period as may be specified in the notice. Failure to comply with the enforcement notice is an offence which, on conviction attracts a fine of 5 million Kenyan shillings or to imprisonment for a term not exceeding two years, or to both. Offences under the Act for which no specific penalty is provided attract upon conviction, a fine of up to 3 million Kenyan shillings and/or a term of imprisonment not exceeding 10 years.

Uganda

Uganda enacted the Data Protection and Privacy Act on 25 February 2019. The Act was benchmarked on the EU data protection regulations and has similar clauses with the GDPR which require strict compliance. Some of the key clauses to note are that; data collectors are required to obtain consent from data subjects, and notify the regulator in case of any breach. Failure to comply or if found in breach of the law, the maximum penalty for companies is 2% of their annual gross earnings.

For individuals, the fine is about Ushs 4,000,000 and/or 10 years' term of imprisonment.

South Africa

The Protection of Personal Information Act (**POPIA**) is South Africa's first comprehensive piece of data protection legislation. The POPIA was originally signed into law in November 2013, the substantive provisions of the law have not yet taken legal effect. Only limited sections of POPIA (predominantly which relate to the office of the Information Regulator) came into effect on 11 April 2014. The remaining provisions of POPIA will come into effect on a date to be determined by the President.

Section 114 of POPIA provides that once the law is fully implemented, its substantive provisions will become enforceable after a one-year transitional period. Part A of Chapter 5, provides for the establishment, duties and powers of the Information Regulator. In line with Part A of Chapter 5, the Information Regulator was established and took office in December 2016. However, POPIA's substantive obligations and penalty provisions are still not in effect because, as outlined by the Information Regulator in a 2016 media statement¹ regarding those provisions, they only can be implemented once the Information Regulator has reached a "stage of operational readiness. Despite POPIA not being fully in effect, the Information Regulator has urged companies to start complying with its provisions ahead of its implementation. The Information Regulator also has written to companies, reminding them of their data privacy obligations once the law does take **effect**.

Nigeria

Nigeria **does not** have a principal data protection law. The Personal Information and Data Protection Bill is pending before the National Assembly. Nigeria has a subsidiary data protection legislation known as the Nigeria Data Protection Regulation (NDPR) 2019 issued by the National Information Technology Development Agency on 25 January 2019.

The NDPR mirrors the GDPR in some respects. It broadens the scope of the regulation to extend to all organisations processing the personal data of natural persons in Nigeria or/ and of Nigerian descent residing in foreign countries. The GDPR widened its regulatory landscape of data privacy to include all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. The NDPR mandates that all public and private organizations in Nigeria, that control data of natural persons, make their respective data protection policies available to the general public within three months after the date of issuance of the Data Protection Regulation. Additionally, all data controllers are always expected to have a Data Protection Officer responsible for ensuring compliance with the provisions of the Regulation.

Egypt

Egypt **does not** have a law which regulates protection of personal data. The Egyptian Parliament is currently discussing the data protection draft law (the "Data Protection Draft Law"), which has been under discussion since 2017 and is expected to be promulgated soon. The draft law is stated to contain provisions relating

to data security, cross-border data transfers and electronic marketing in the draft law. Under the draft law, personal Data may not be collected, processed or disclosed, without the explicit and rescindable consent of the Data Subject.

Ghana

The primary legislation governing privacy/ data protection in Ghana is the Data Protection Act, 2012 ([Act 843](#)). The Act establishes the Data Protection Commission whose role is to protect the privacy of the individual and personal data by regulating the processing of personal information. The Act provides that personal data shall not be processed without the prior consent of the data subject. Where the personal data of a data subject has been accessed or acquired by an unauthorised person, the data controller or a third party who processes data under the authority of the data controller shall notify the Commission and the data subject of the unauthorised access or acquisition as soon as reasonably practicable.

Failure to comply with an enforcement notice attracts a fine of not more than one hundred and fifty penalty units or to a term of imprisonment of not more than one year or to both. Commission of an offence under the Act for which no penalty is prescribed attracts a fine of not more than 5000 penalty units or a term of imprisonment not more than 10 years or both.

ARTIFICIAL INTELLIGENCE SYSTEMS

There have been a number of developments

over the past two years that point to a growing AI scene across the region. Local AI labs and research centres have appeared throughout Africa, such as the announcement in June 2018 that [Google](#) was to open their first African AI research hub in Accra, Ghana. Progress in AI in Africa is likely to be led by the [private sector](#) due to lack of funding and a limited AI-skilled workforce in most government institutions. Leading AI companies like Google and Facebook are moving at a much faster pace in AI development than most African governments are. These companies will be part of policy formulation process with other stakeholders. There is no well-documented strategy for AI in Africa as there is in Europe, Canada, the U.S., and China. There is also a lack of systematic data on AI progress in Africa.

This section focuses on legislative progress in Kenya, South Africa, Tunisia, Nigeria, Uganda and Ghana. These countries are currently among the only 12 placed African governments in the top 100 of Government AI Readiness index 2019.

Currently only two African nations have adopted national AI strategies - Kenya and Tunisia. The Kenyan government created a Blockchain & Artificial Intelligence [task force](#) in February 2018.

The first goal of the group is to provide the government with recommendations about how to harness these emerging technologies over the next five years. Tunisia has created an AI [Task Force](#) and Steering Committee to develop a national AI strategy.

Nigeria

In the case of Nigeria, there is the National Agency for research in Robotics and Artificial Intelligence ([NARRAI](#)) whose focus is to train Nigerians to use skills in AI to quicken the country's economic growth. Whether this approach can be accounted as strategy is questionable?

South Africa

South Africa has not yet formalised any policy documents or entered bills to parliament for the regulation of AI. However, in April 2019, the President appointed members to the Presidential Commission on the Fourth Industrial Revolution (4IR Commission), which will assist the government in taking advantage of the opportunities presented by the digital industrial revolution. The task of the [4IR Commission](#), which will be chaired by the President, is to identify relevant policies, strategies and action plans that will position South Africa as a competitive global player. This suggests that the government is committed to adopting strategies to equip South Africa for the Fourth Industrial Revolution.

Uganda

In Uganda, the National [Taskforce](#) on 4ir was launched by the President on April 8, 2019. Currently, Uganda is working on its National 4ir strategy which is a broad based approach to harnessing blockchain, Artificial intelligence, cyber security, drones et al. Uganda is one of the only 12 counties in the 2019 top 100 Government AI readiness index.

BLOCKCHAIN

Blockchain is a revolutionary technology that

allows parties to transact [directly](#) with each other without the need for intermediaries, as central trusted third parties. Cryptocurrency is the most popular example that is intrinsically tied to blockchain technology. It is also the most controversial one. Nonetheless, blockchain technology itself is non-controversial, and has worked flawlessly over the years and is being successfully applied to both financial and non-financial applications.

Botswana

The Bank of Botswana has not released any regulation on [cryptocurrencies](#) or the use of blockchain technology and has reportedly stated that it currently has no intention of regulating cryptocurrencies. The use of cryptocurrency and blockchain technology in Botswana is being driven by the Private sector.

Ghana

The Bank of Ghana has [announced](#) that the trading and use of cryptocurrency in Ghana is not yet legal because it is not recognized as a legitimate form of currency. This is because all media of exchange in the country must be supported by the Bank of Ghana, which has not yet approved the use of cryptocurrencies.

However, the Bank of Ghana has drafted a Payment Systems and Services Bill (Ghanaian Bill), which it believes will enable the regulation of cryptocurrency in Ghana in the future. After a preliminary review of the Ghanaian Bill, there seems to be no reference to cryptocurrency, blockchain or digital currency, however cryptocurrencies will apparently be regulated through companies registered with the government as "Electronic Money Issuers." The Bank of Ghana has discouraged

the use of cryptocurrency until the promulgation of the Ghanaian Bill.

Kenya

Kenya does not yet have a blockchain [regulatory](#) framework in place. The Central Bank of Kenya issued a warning on the use of cryptocurrencies in 2015 due to their perceived volatility and lack of specific governing legislation. Despite this [warning](#), interest in cryptocurrencies continues to gain significant momentum, with fintech ventures such as BIT-PESA leveraging on Bitcoin technology to effect payments.

On 28 February 2018, the Kenyan government (through its ICT Cabinet Secretary) announced that it would appoint an 11-member task force to explore the use of distributed ledger technology and artificial intelligence. This comes after the President of Kenya announced his intentions for Kenya to explore the opportunities in the new technology found in the fourth industrial revolution.

Nigeria

In early 2017, the Central Bank of Nigeria [warned](#) financial institutions not to use, hold or trade virtual currencies pending substantive regulation or decision by the (Central Bank of Nigeria) as they are not legal tender in Nigeria. A circular was released by the Central Bank of Nigeria prohibiting the trading of cryptocurrencies by financial institutions in Nigeria. However, the Nigerian senate has launched an investigation into "the viability of bitcoin as a form of payment". The slow acceptance of cryptocurrencies by the regulators is notable considering that Nigeria is reportedly the third largest holder of bitcoin in the world.

Uganda

The United Nations African Institute for the Prevention of Crime and the Treatment of Offenders ([UNAFRI](#)) together with the University of Birmingham Law School, hosted a round table discussion in 2016 with Ugandan members of Parliament, regulators and academia to discuss the regulation of cryptocurrencies in Uganda (the UNAFRI Meeting). It was reportedly agreed at the UNAFRI Meeting that Uganda's legislation, in its current state, does not govern the use of cryptocurrencies. Further, it was determined that cryptocurrency does not fall under the definition of fiat currency in terms of the Bank of Uganda Act, 2000. In February 2017, the Bank of Uganda issued a warning to the general public about One Coin Digital Money, a Bulgarian company operating in Uganda, and cautioned that "whoever wishes to invest their hard-earned savings in cryptocurrency forms ... is taking a risk in the financial space where there is neither investor protection nor regulatory purview."

On 28 May 2020, The National Payment Systems Bill was passed into law by parliament waiting to be assented by the President. The bill defines Electronic money as monetary value represented by a claim on the issuer, which is stored on an electronic device. Although the bill doesn't expressly mention the terms blockchain or cryptocurrency, the definition of electronic money covers the two. The Act also provides for licensing of payment service provider as an electronic issuer. A payment service is defined as any other service incidental to the transfer of funds. It therefore appears that once enacted, the National Payment Systems Act will regulate the

Act will regulate the transfer of cryptocurrency as form of payment.

South Africa

In December 2014, the South African Reserve Bank (SARB) [issued](#) its position paper on virtual currencies whereby it confirmed that the SARB has the sole right to issue legal tender and that decentralised convertible virtual currencies do not constitute legal tender in South Africa.

As a result of the growing interest and rapid innovation in the financial technology ("fintech") and crypto assets domain, the Intergovernmental Fintech Working Group ("IFWG") was established in 2016. In early 2018, a joint working group, the Crypto Assets Regulatory Working Group (the "CARWG") was established under the aegis of the IFWG. The mandate of the CARWG was to review the position on crypto assets and to consider the public policy concerns raised by these assets, which should inform the regulation of these assets going forward. In January 2019, the IFWG and the CARWG released a joint consultation paper titled the "Consultation Paper on Policy Proposals for Crypto Assets" (the "Consultation Paper") for public comment. While the Consultation Paper identified the following crypto asset specific use cases, it currently focuses only on the purchase and sale of crypto assets and payment using crypto assets. The regulatory authorities in South Africa are of the view that [crypto assets](#) do not constitute "money" as per the traditional definition of the word, but acknowledge that crypto assets may perform certain functions similar to those of currencies, securities and commodities. There is currently no fintech specific regulation for

crypto assets, but crypto assets are also not prohibited.

CRYPTO ASSETS UNDER TAXATION LAWS

Under the VAT Act 89 of 1991, it is proposed to [amend](#) section 2 to include in the description of "financial services", the issue, acquisition, collection, buying or selling or transfer of ownership of any crypto assets. As a result, if the proposal in respect of the VAT Act is accepted, all dealings in crypto assets will be exempt from VAT in terms of section 12 of the VAT Act. Under the Income Tax Act, it is proposed that crypto assets be included in the definition of "financial instrument". The purpose of these proposed amendments to the tax legislation is to clarify the tax treatment of crypto assets under the tax laws. From an income tax perspective, crypto assets are to be treated as financial instruments for income tax purposes, and from a VAT perspective, the issue, acquisition, collection, buying or selling or transfer of ownership of any crypto asset is to be treated as a financial service.

Zambia

In October 2018, the Bank of Zambia released a [press statement](#) on the use of cryptocurrencies in Zambia. The Bank of Zambia confirmed that cryptocurrencies "are not legal tender in Zambia" and confirmed that in terms of section 30 of the Bank of Zambia Act (Chapter 360 of the Laws of Zambia), the Bank of Zambia is the only body with the right to issue notes and coins and as it has not issued any form of cryptocurrency - cryptocurrencies are not legal tender in the Republic of Zambia.

Egypt

The Central Bank of Egypt issued a **warning** in January 2018 against the trading of cryptocurrencies, such as bitcoin, due to extremely high risk associated with such currencies. The Central Bank also asserted that commerce within the Arab Republic of Egypt is confined only to the official paper currencies approved by the Bank. Egypt's Dar al-Ifta, the primary Islamic legislator in Egypt issued a religious decree classifying commercial transactions in bitcoin as *haram* (prohibited under Islamic law).

In May 2019, the Central Bank of Egypt announced it is working on a draft law for crypto-related activities which will oblige financial institutions in the country to obtain licences in advance for issuing and trading of cryptocurrencies.

DIGITAL IDENTITY

Overview

The United Nations' Sustainable Development Goals (SDGs) aim for every person to have a legal identity by 2030 according to SDG 16.9. Currently, over 1.5bn people **lack** any form of legally recognised identity and this disproportionately impacts rural residents, poor people, women, children, and other vulnerable groups in Africa. The best way to achieve this goal is through **digital identity** (digital ID) systems, central registries storing personal data in digital form and credentials that rely on digital, rather than physical, mechanisms to authenticate the identity of their holder. As the advance into the digital age where more transactions take place online, the ability to prove a unique identity in the virtual world, as well as the analogue world, becomes increasingly

important for economic and social inclusion.

Digital ID is a means of identifying or authenticating the identity of an individual both online and offline.

However, majority of the countries in Africa lack adequate legal frameworks to support and regulate modern identity management systems. They lack sufficient regulations to protect personal data and uphold individual rights to privacy and fair use of data. These countries include Rwanda, Zambia. Other countries have draft laws on data protection that are currently not in force. These include Botswana, Nigeria, South Africa, Egypt and Tanzania. Only Uganda, Kenya, Ghana, have adequate legal frameworks and authorities to protect personal data.

In addition, many identity related laws are **outdated** and do not take into account the digital nature of modern data capture, storage and use.

Kenya

Kenya enacted into law the Statute Law (Miscellaneous Amendment) Act No. 18 of 2018. The effect of the Act was to **amend** several provisions of the Registration of Persons Act (Cap 107 Laws of Kenya). The amendments to the Registration of Persons Act established a National Integrated Information Management System (hereinafter "NIIMS") also known as Huduma Namba that is intended to be a single repository of personal information of all Kenyans as well as foreigners resident in Kenya. The system, created under section 9A of the Registration of Persons Act, is designed to collect biometric and demographic data, including deoxyribonucleic acid (DNA) and

geographic positioning system (GPS) coordinates. However, concerns raised about the invasiveness and surveillance potential of the system led to Kenya's high court temporarily suspending the country's new national biometric identity program until the government enacts laws to protect the security of the data and prevent discrimination against minorities. The government will now have to pass new legislation under public scrutiny to build in protections and implement the biometric program. At the time of the suit, Kenya had not yet enacted the Data Protection Act on 8 November 2019 establishing requirements for protection of personal data.

Uganda

The Registration of Persons Act 2015 saw the creation of the National Identity and Registration Authority (NIRA) to oversee all foundational identity infrastructure, resulting in the creation of the new electronic national identity card. Uganda seeks to integrate government services and databases with the central national identity database.

Uganda enacted the Data Protection and Privacy Act on 25 February 2019. The purpose of the Act is to protect the privacy of the individual and of personal data by regulating the collection and processing of personal information; the Act provides that the data controller/processor should be accountable to the data subject for the data collected.

Ghana

The National Identification Authority ([NIA](#)) was set up in 2003 under the Office of the President with the mandate to issue national ID cards and manage the National Identifica-

tion System (NIS). This resulted in the passing of the National Identification Authority Act, 2006 (Act 707) to give it the necessary legal premises on which to operate. The National Identity Register Act, 2008 (Act 750) was also passed to give authorization for collection of personal and biometric data and to ensure the protection of privacy and personal information of enrollees/applicants.

The Data Protection Act, 2012 establishes a Data Protection Commission, to protect the privacy of the individual and personal data by regulating the processing of personal information, to provide the process to obtain, hold, use or disclose personal information and for related matters.

About the authors

Alice Namuli is a leader of legal innovation across Africa. She is head of technology and



innovation at a top tiered African law firm, and founder of the Legal Innovation Hub in Uganda, as well as a host and ambassador of the World Legal Summit.

Bachelors of Law from Makerere University, has a background in policy research, and is a writer for the Legal Innovation Hub in Uganda.

Collins Tumukunde has recently received his

WLS IN ACTION





WLS Portugal



WLS Kenya at Lawyers Hub





Regulatory Developments in AI, Decentralised Technologies, Data Protection and Cybersecurity in the Asia-Pacific

By David N. Alfred, Director and Co-Head of the Data Protection, Privacy and Cybersecurity Practice at Drew & Napier LLC and Josh Lee Kok Thong, Chair of the Asia-Pacific Legal Innovation and Technology Association, and WLS Ambassador for Asia

In this article, we give an overview of legislative developments relating to the regulation of AI and decentralised technologies, as well as in relation to data protection and cybersecurity generally in the Asia-Pacific region. AI to Asia might be what steam power was to Europe - a technology that dramatically transforms the fabric of society.

The use of data has seen significant growth over the last ten years. Many businesses are seeking to leverage the vast amounts of data they have collected, often from their customers or their commercial activities and operations. This has contributed to the adoption of new technologies such as artificial intelligence (AI) and blockchain, as well as increased concerns about the protection of data, including personal data, and information systems. In this article, we give an overview of legislative developments relating to the regulation of AI and decentralised technologies, as well as in relation to data protection and cybersecurity generally in the Asia-Pacific region.

AI

AI to Asia might be what steam power was to Europe - a technology that dramatically transforms the fabric of society. While such transformation will certainly not be limited to Asia, AI products and services are being introduced across strategic industries driving the economic dynamism of emerging and developed Asian economies (like finance, healthcare, retail, transport, manufacturing and agriculture). AI adoption may still be nascent, but the understanding of its potential certainly is not.

The growth of AI, however, brings complex and multifaceted challenges to the fore. Key issues include:

1. **Infrastructure:** Strong infrastructural foundations providing reliable and widespread connectivity are needed to build digitally innovative economies. When these are not available (which continues to be the case in many parts of Asia), individuals and businesses lose the opportunity to gain

and contribute to such ecosystems.

2. **Access to data:** As key drivers of digital products and services - and practically the lifeblood of modern AI systems - data needs to be able to flow freely and securely across platforms, along with robust ways of collection, processing and transfer. This is covered more fully in an earlier subsection.
3. **Skills and human capital:** Workers with technical skills and knowledge are needed to ensure that no one gets left behind as industries turn towards automation.
4. **Trust and partnerships:** Developing AI in a safe, ethical and sustainable manner can increase societal trust and understanding, which in turn improves the pace and scope of AI adoption.
5. **Ecosystem and entrepreneurship:** Local AI industries are needed for economies to remain relevant and competitive in the age of AI. This requires the right enabling regulatory and policy frameworks to support the growth of national AI value chains.

In particular, the issue of regulation and building trust has been gaining significant attention. Conversations are ongoing about developing frameworks to ensure that AI systems are fair, transparent and inclusive, and rooting these frameworks in local, regional and international collaboration schemes that enable best practices, standards and principles to be shared.

So far, there are no specific laws governing the ethical use of AI around the region. Nevertheless, as one can see below, efforts are under way to better understand and address legal, moral and ethical issues raised by the adoption of AI systems and services. Notable examples include:

- **Australia:** The Commonwealth Scientific and Industrial Research Organisation launched a landmark discussion paper on a proposed ethics Framework. The paper highlights eight core principles to guide AI deployment in the Australian economy: generating net benefits, doing no harm, complying with regulatory and legal requirements, appropriately upholding privacy, boosting fairness, being transparent and easily explained, containing provisions for contesting a decision made by a machine, and including an accountability trail.
- **China:** In 2019, China released the Beijing AI Principles, a code of ethics for AI aiming to guide AI scientists and engineers as they research, develop, use and plan AI-based systems. China also released (in 2018 and 2019 respectively) White Papers on AI Standardisation and AI Security Standardisation, which seek to (among other things) improve security, ethics, and privacy-related standards, laws and policies.
- **Japan:** The Ministry of Economy, Trade and Industry (METI) formulated the “Contract Guidance on Utilisation of AI and Data” to help organisations navigate the complexities of drafting a contract that involves AI-and data-based systems. METI is also looking to develop guidelines to ad-

dress issues such as legal liability and user rights. The Ministry of Internal Affairs and Communications has also held a series of conferences which saw the release of Japan’s “AI R&D Guidelines” in 2017 and “AI Utilization Guidelines” in 2019. Following intergovernmental and multi-stakeholder discussions, the Cabinet Secretariat also released the “Social Principles of Human-Centric AI” in February 2019.

- **Singapore:** The Personal Data Protection Commission (PDPC) and Info-comm Media Development Authority released (in 2019 and 2020 respectively) the sector-agnostic Model AI Governance Framework and the Implementation and Self-Assessment Guide for Organisations, which translate ethical principles into practical recommendations to help organisations adopt responsible AI governance. In 2018, Singapore also established the Advisory Council on the Ethical Use of AI and Data and the Research Programme on the Governance of AI and Data Use, to guide governmental thinking on dealing with long-term, complex policy and regulatory challenges. Sector-specific initiatives include the Ministry of Transport’s Committee on Autonomous Road Transport, which will look into regulating the use of driverless cars in the near future. In 2018, the Monetary Authority of Singapore also released the “Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore’s Financial Sector”.

The lead taken by the countries above in ad-

dressing issues of fair and accountable AI systems from a policy and regulatory perspective will act as useful resources for other governments as they formulate their own AI strategies.

Regulation and governance, however, cannot happen in a vacuum.

While AI research and development races ahead, with regulation and governance discussions following behind, more remains to be done in encouraging adoption. In this regard, countries in the region have also taken steps to encourage widespread adoption of AI through various national strategies. For example, China and Singapore have broad, overarching national policies designed to drive AI readiness and regulate its deployment. In particular, Singapore set up the National AI Office to oversee the implementation of its National AI Strategy (which was announced in November 2019). Malaysia and South Korea have included AI within broader digital transformation plans. Indonesia and Thailand have launched target initiatives and programs to facilitate the adoption of AI systems in strategic sectors and industries, focusing on public-private cooperation to drive adoption. Indonesia is also looking to create its own national AI strategy. Lastly, while Australia has no formal AI policy in place, it has a variety of official guidelines, principles and standards to help individuals, businesses and institutions prepare for AI-drive disruption.

A summary in these few paragraphs cannot hope to do a semblance of justice to the multitude of initiatives and programs to foster AI innovation, regulation and adoption in Asia. It

suffices to say these are merely the introductory chapters to what promises to be an exciting future for AI in Asia.

Decentralised Technologies

Distributed ledger technology (DLT), the underlying technology for blockchain, crypto assets and initial coin offerings, creates new opportunities and challenges for the development of the financial sector in Asia. While DLT applications have raised hype, volatility and concerns, DLT is expected to find more applications and, in the longer term, fundamentally transform economic and financial systems.

To understand the field of DLT, blockchain, and related applications, we begin with the relevant underlying technology. A “distributed ledger” is a digital database that is shared, independently updated, and synchronized by consensus among the network participants. Data storage points (nodes) are connected with each other and store all data simultaneously by consensus, and together constitute the common ledger. DLT systems thus offer the potential for greater security without the risks of concentration of centralised ledger systems. They, however, typically suffer in speed of execution as a result of such decentralisation.

Given its nature and properties, DLT provides trust solutions involving enhanced security, transparency, and permanence, with applications in (among other things) asset finance, back office clearing and settlement, trade processing and settlement, insurance claims tracking, cross-border remittances,

internet of things, smart contracts, and digital identity instruments.

However, it is generally becoming clear that the promises of DLT are not universally true.

The key attributes of DLT (security, transparency, and permanence) are not absolute or as strong as suggested. As Zetzche, Buckley and Arner note in 2018, “risk does not vanish if financial services are provided via distributed ledgers”. DLT and blockchain may enhance efficiency (e.g., by making it more difficult to tamper with the stored data), but the underlying risks do not disappear entirely: DLT does not necessarily make data tamper-proof (although blockchain can make data tamper-evident). Specific features of DLT may also multiply some existing risks and even give rise to new risks. These include:

1. **Transparency:** The key idea behind DLT - that the same data is distributed among all data nodes - promotes transparency as well as security. This, however creates complications whenever parts of shared data are of a confidential nature. Even where data on a DLT does not reveal the identity of a person, there is a risk that information from a user’s profile can be used to re-identify the person. In fact, re-personalization of pseudonymous data on distributed ledgers has already become a business, with companies offering data-tracking services.
2. **Cyber risks:** DLT does not immediately reduce cyber risks, and in some cases even enhances them. First, inaccurate sets of data distributed across a distributed net-

work will remain inaccurate, and its visibility across the network may increase the likelihood that others may act upon such data. Second, DLT offers increased safety of data compared to a centralized ledger only when the cybersecurity of the central node of the centralised ledger is lower than the resilience of such number of nodes that is sufficient to establish a consensus of the entire distributed ledger. That is however not always true, with centralised ledgers often employing some of the most robust cybersecurity measures.

3. **Operational risks:** Any errors in the code implemented on the ledger are replicated across the entire network. When mistakes happen or the expectations associated with the increased efficiency of DLT are not met, questions arise as to who bears legal responsibilities.

Notwithstanding the risks above, the main regulatory challenge for the applications of DLT lies in its multifaceted nature. As variations of DLT can be applied across a financial system, the regulatory response thus far has been limited. In Asia, some governments are attempting to provide a firm legal basis for distributed ledgers by implementing the corresponding definitions by virtue of statute. Others focus specifically on blockchain. The majority, however, are silent on the matter of bespoke regulation of either component of DLT.

This does not mean, however, that DLT systems operate in a legal vacuum. Regulators and lawyers are already applying existing legal constructs and principles, including corporate, contract, tort, and property law.

In *B2C2 v Quione* [2020] SGCA(I) 02, for instance, the Singapore courts relied on contractual principles of unilateral mistake and breach of contract to rule on a case involving the autonomous algorithmic trading of digital tokens. In the absence of international rules, it is likely that jurisdictions will continue to approach the matter in different ways.

Another regulatory challenge is terminology. Attempts to regulate DLT have been fraught with problems of terminology, especially in jurisdictions aiming to establish special rules for blockchain. The latter concept has proven particularly difficult to define with sufficient accuracy, culminating in new rules that are not only overly simplistic, but also confusing and even misleading.

The apparent confusion of some lawmakers and hesitation of others can be explained, at least in part, by the lack of accepted international terminology and the absence of agreed standards to define DLT. It remains to be seen whether attempts such as the ISO/CD 22739 “Blockchain and distributed ledger technologies - Terminology” will be able to address these issues.

To address the regulatory issues above, the Asian Development Bank has proposed the following approach:

1. Policymakers and regulators should treat DLT as a platform technology which can be used across a wide variety of functional areas.
2. A general system of categorisation and certification should be developed on an

industry basis, e.g., through the ISO.

3. Regulatory treatment should vary depending on the context. Presently, the focus should be on regulating the applications of DLT associated with the biggest risks (such as crypto assets and initial coin offerings).
4. Emphasis should be placed on the role of intermediaries, as this is where the greatest risks exist (with digital asset exchanges the most urgent focus of attention, to address risks of market integrity, consumer protection, and financial stability).
5. Policymakers and regulators should strive to better understand individual use cases and systems. This requires massive investment in technology and innovation expertise.

While DLT continues to face many significant operational and regulatory challenges, its potential to transform financial and economic systems - especially many in Asia, which sometimes suffer from reliability and trust concerns - is significant. This remains an exciting regulatory space to watch.

Data Protection

Another area which is experiencing significant (one might even say, exciting) change across the Asia-Pacific is data protection. Data protection laws generally seek to protect individuals’ personal data or, more specifically, their privacy with respect to such data.

Such laws typically include requirements relating to consent, notification of purposes,

processing of personal data, data quality and security of personal data, as well as various rights of individuals in relation to their data. Such laws typically include requirements relating to consent, notification of purposes, processing of personal data, data quality and security of personal data, as well as various rights of individuals in relation to their data.

Data protection laws first appeared in Europe in the late 1970s and the most significant recent development there was the enactment of the General Data Protection Regulation in 2016. Much of the Asia-Pacific has lagged behind Europe for many years in enacting laws to protect individuals' personal data. This has changed significantly in the last 10 years or so with several jurisdictions enacting new data protection legislation or updating existing legislation. These include, for example, Australia (1988, amended 2014 and 2018), Hong Kong (1995, updated 2013), Japan (2003, amended in 2016), Malaysia (2010), Taiwan (2010), South Korea (2011, updated 2020), the Philippines (2012), Singapore (2012) and China (2017).

Nevertheless, developments continued unabated through 2019 and into 2020. The following is a short list of the more significant developments:

New Data Protection Laws

- **Thailand** enacted and published a new law on data protection, the Personal Data Protection Act (2019), in May 2019. This law incorporates many of the common data protection principles, such as the lawful bases for processing personal data, consent, notification of purpose, security

obligations and requirements for cross-border data transfers. The law also includes provisions on mandatory data breach notification. The new law was due to come into force in May 2020 but this has been postponed to May 2021 due to the COVID-19 outbreak.

- **Vietnam** announced in mid-2019 that it would enact a new Decree (law) on personal data protection and the first draft of the Decree was published in late December 2019. The draft Decree sets out 7 data protection principles covering the lawfulness, purpose for collection and use of personal data, as well as data quality, amongst others.
- In **India**, the Personal Data Protection Bill was tabled in its Parliament in December 2019. It contains provisions (and penalties) which are similar to the GDPR, including provisions on mandatory data breach notification, data portability and a right to be forgotten, though there are significant differences as well. Notably there are data localisations and data "mirroring" requirements (which are seldom, if ever, found in data protection laws) and also criminal penalties for certain contraventions. While this is a significant development, it is not clear when the Bill may be enacted into law.

Reviews of Existing Data Protection Laws

- **Malaysia** issued a public consultation in February 2020 to seek views on possible changes to its Personal Data Protection Act.

Among the proposed changes are a right to data portability, mandatory data breach notification, a requirement to appoint a data protection officer and a duty to implement privacy by design.

- **Japan** announced in March 2020 that it intends to make various amendments its Act on the Protection of Personal Information (APPI) to strengthen the rights of individuals and the protection of personal information generally. Notably, the amendments include provisions on mandatory data breach notification, restriction of unlawful use, use of pseudonymised information and requirements for overseas transfers of personal information.
- **Hong Kong** published a discussion paper on proposed amendments to its Personal Data (Privacy) Ordinance in January 2020. Among the proposed changes are a mandatory data breach notification mechanism, provisions on data retention period and changes to the fines and penalties which may be imposed for contraventions.
- **Singapore** recently (in May 2020) issued a public consultation on a draft Bill to amend its Personal Data Protection Act 2012 (PDPA). Key amendments include new provisions on mandatory data breach notification, data portability, processing of personal data for legitimate purposes and a new offence relating to unauthorised re-identification of anonymised information, amongst others. The draft Bill also increases the maximum financial penalty which may be imposed for a contravention to 10% of the organisation's annual turnover or

S\$1 million, whichever is higher. Separately, following Singapore's accession to the APEC Cross-border Privacy Rules (CBPR) system and Privacy Recognition for Processors (PRP) system in 2018, Singapore has also recently amended its Personal Data Protection Regulations 2014 to expressly permit transfers of personal data to overseas organisations which have been certified under the APEC CBPR or PRP systems.

- In **New Zealand**, a Privacy Bill is currently making its way through the New Zealand Parliament, with its first reading there in April 2018 and its second reading in August 2019. The Privacy Bill will replace New Zealand's existing Privacy Act 1993 and is intended to "modernise" the law. Significant changes include clarification on when the law applies to overseas organisations (depending on what business they carry on in New Zealand), notification of privacy breaches and requirements for transfers of personal data outside New Zealand, amongst others.
- In **Australia**, the government is conducting a review of its Privacy Act 1988, to be completed in 2021.

Data protection continues to be a key concern in many jurisdictions as new technologies (including AI and blockchain) enable the collection and processing of vast amounts of personal data and new approaches are required to address the risks which arise. This concern is motivated in some cases by increasing consumer concerns over the protection of personal data. There are also significant economic

reasons for ensuring that the legal framework for data protection enables the meaningful collection, use and disclosure of personal data, both within and across national borders, while affording an appropriate standard of protection.

Cybersecurity

The landscape of cybersecurity laws across the Asia-Pacific is very different as there are far fewer countries which have enacted laws aimed specifically at cybersecurity (that is, apart from laws generally relating to IT, electronic transactions or cybercrime) and the scope of such laws varies considerably. Some cybersecurity laws share similarities with data protection laws as both types of laws are, to some extent, concerned with the security of data, there may be similar requirements under both, for example, in relation to the types of security arrangements which organisations are required to implement or data breach notification requirements. Perhaps the most notable example of this overlap is China's Cybersecurity Law, which includes provisions relating to both cybersecurity and data protection. Some of the more recent laws in the Asia-Pacific on cybersecurity are found in Singapore (2018), Taiwan (2018), Vietnam (2018) and Thailand (2019).

While laws relating to cybercrime have existed in various jurisdictions for many years, the cybersecurity threat landscape has changed significantly in recent times. Cybersecurity risks have increased sharply with attackers becoming more sophisticated and adept at finding and exploiting weaknesses in the protection of information systems.

A key focus of Singapore's Cybersecurity Act 2018 and Thailand's Cybersecurity Act 2019 is the protection of "critical information infrastructure", which generally refers to computer systems which are necessary for the provision of certain essential services (Singapore) or which relate to certain national functions or are in the public interest (Thailand). Protection of critical information infrastructure is of significant national concern in these countries and the laws place various obligations on the operators of such infrastructure to address and mitigate the effects of a cybersecurity attack.

While some may question the need for such laws, requirements to implement security measures to protect personal data have existed for many years. The experience under data protection laws suggest that there is a role to play in ensuring that organisations proactively take the necessary measures to protect information systems and the data they contain.

About the Authors

David N. Alfred is Director and Co-Head of the Data Protection, Privacy and Cybersecurity Practice at Drew & Napier LLC in Singapore.



David N. Alfred

He is also Co-Head and Programme Director of the Drew Data Protection & Cybersecurity Academy.

Josh Lee Kok Thong is the Chairperson of the Asia-Pacific Legal Innovation and Technology Association. He is also the co-founder of Law-Tech.Asia, and law and technology virtual publication based in Singapore.

In this article, we give an overview of legislative developments relating to the regulation of AI and decentralised technologies, as well as in relation to data protection and cybersecurity generally in the Asia-Pacific region.



Josh Lee Kok Thong

WLS IN ACTION









EUROPEAN SUMMARY

By Federico Gabbricci, Researcher at The Thinking Watermill Society and Deborah Bolco, Partner of Pavia e Ansaldo Law Firm

Digital technology is changing people's lives, and it is bringing new challenges. The European Commission, to deal with these challenges, has adopted, on 21 November 2018, a digital strategy which sets a vision for the Commission to become a digitally trans-

formed, user-focused and data-driven administration by 2022.

In the next pages, we are going to introduce the main themes of digital transformation, highlighting how the European Institutions are dealing with them.

DECENTRALIZED SYSTEMS

Blockchain

Blockchain technology is increasingly becoming the focus of European Institutions. The importance of this technology was highlighted in the *European Parliament resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation*. The resolution highlighted the wide range of DLT-based applications that could potentially affect all sectors of the economy such as energy, transport, healthcare, supply chains, education, as well as the financial sector.

Furthermore, the resolution invited the European Commission not only to try to remove existing barriers preventing the implementation of blockchains but also to assess and develop a European legal framework and to develop common initiatives to raise awareness and train citizens, businesses and public administrations to facilitate the comprehension and uptake of this technology.

Also, in 2018, the European Commission has launched the **EU Blockchain Observatory and Forum**, with the purpose of mapping key initiatives, monitoring developments and inspiring common actions.

The Observatory, in 2019, has published a report "*Legal and regulatory framework of blockchains and smart contracts*", commissioned by the European Union, where it addressed the issues about whether or not blockchain technology needed to be regulated. The study focused on the reasons why

blockchain must be ruled. The reasons are intrinsic to one of the main features of blockchain technologies: the decentralization. The result of this feature is the difficulties to identify blockchain's users and the a-territoriality of the blockchain (considering that nodes can be located in different jurisdictions). For these reasons, the Observatory stressed the importance to create a *<<predictable legal and regulatory framework>>* and provided eight guiding principles to aid policymakers in dealing with these and other questions:

1. Craft simple yet usable definitions of the technology.
2. Communicate legal interpretations as broadly as possible.
3. Choose the right regulatory approaches for the question at hand.
4. Harmonize the law and interpretations of it.
5. Help policymakers develop an understanding of the technology.
6. Work on high-impact use cases first.
7. Closely monitor developments in less mature use cases and encourage self-regulation.
8. Make use of blockchain as a regulatory tool.

Finally, it is worth noting the signing of the **European Blockchain Partnership** between the European Member States. This initiative wants to promote the cooperation between the States to exchange experience and expertise about the blockchain.

Furthermore, the Partnership set itself the objective to build a European Blockchain Services Infrastructure which will deliver EU-

wide cross-border public services using blockchain technology.

If we add to this the increasing interest of the private sector about the blockchain, we can determine that very soon blockchain technology will be widespread in all of the European Union.

Smart Contracts

A smart contract is a computerized protocol which automatically executes contract terms when certain conditions (predetermined by the contracting parties) are fulfilled.

Smart contracts are linked with blockchain technology. The blockchain allows for the notarizing of the will of the parties, enabling the univocal identification of the seller, the buyer and the bargaining chip. As soon as the smart contract is recorded in the blockchain, the instructions given by the parties and their planned actions become irrevocable and non-editable.

The European Parliament, in the resolution of 3 October 2018 “*on distributed ledger technologies and blockchains: building trust with disintermediation*”, it has been stated that the European Commission needs to undertake an in-depth assessment of the potential for and legal implications of smart contracts. Moreover, the resolution has emphasized that legal certainty surrounding the validity of a digital cryptographic signature is a critical step towards facilitating smart contracts. In addition, the European Parliament has called on the Commission to promote the development of technical standards with rele-

vant international organizations such as ISO, ITU and CEN-CELENEC, and to conduct an in-depth analysis of the existing legal framework in the individual Member States concerning the enforceability of smart contracts.

Finally, the European Parliament invited the Commission to pursue an enhancement of smart contracts through legal coordination or mutual recognition between the Member States.

Cryptocurrencies

Cryptocurrencies are digital coins, used, if agreed between the parties, as a medium of exchange to purchase goods and services. It is transmitted, archived and negotiated electronically using blockchain technology.

According to the **European Central Bank**, cryptocurrencies are not a currency because they are not issued by a Central Bank. For the ECB they are just a speculative asset.

Also, cryptocurrencies mustn't be classified as electronic money under the Directive 2009/110/EC because:

- They are not issued by any central public authority
- They are not a generally accepted form of payment
- Users are not protected by an appropriate regulatory framework
- They are too volatile

The cryptocurrencies have been partially ruled by the **IV Anti Money Laundering Directive** (EU Directive 2015/849). The directive

has extended the rules on combating money laundering and terrorist financing to virtual currency exchange platforms and custodian wallet providers. In this way, the European legislator has deleted a grey area which allowed terrorist organizations to transfer money anonymously, using cryptocurrencies, through the European financial services.

AUTONOMOUS SYSTEMS

Artificial Intelligence

The European Commission, in the *Draft of Ethical Guidelines for trustworthy AI*, has given the following definition of Artificial Intelligence: <<Artificial intelligence (AI) refers to systems that display intelligent behavior by analyzing their environment and taking actions, with some degree of autonomy, to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications).>>

In February 2020 the President of the European Commission Ursula von der Leyen presented the "*White Paper on Artificial Intelligence: a European approach to excellence and trust*" in which the positions, the goals and the approach of the Commission about the developments of the AI were defined.

With reference to the future regulatory framework, the Commission proposed to follow a risk-based approach to ensure a propor-

tionate regulatory intervention. The idea of the Commission is to distinguish between high-risk AI and no high-risk AI. The Commission believes that a given AI application should generally be considered high-risk in light of what is at stake, considering whether both the sector and the intended use involve significant risks, in particular from the viewpoint of protection of safety, consumer rights and fundamental rights.

With regard to the legal requirements for the **high-risk AI applications** they could consist of the following key features:

- training data of the AI systems in order to respect the EU's values and rules, specifically concerning safety and existing legislative rules for the protection of fundamental rights;
- keeping of records about the programming of the algorithm and data used to train high-risk AI systems in order to allow potentially problematic actions or decisions by AI systems to be traced back and verified;
- information provision about the use of high-risk AI systems regarding particularly system's capabilities and limitations;
- robustness and accuracy of the AI systems in order to ensure their development responsibly and with an ex-ante due and proper consideration of the risks that they may generate;
- human oversight in order to ensure that an AI system does not undermine human autonomy or cause other adverse effects; and
- specific requirements for certain particular AI applications, such as those used for purposes of remote biometric identification.

On the contrary, regarding the **not high-risk AI applications**, they will continue to be covered by the current legislation on product safety (*General Product Safety Directive*; *Product Liability Directive*) and by the legislation on protection of personal data (*General Data Protection Regulation*).

Furthermore, the European Commission in the White Paper stressed the need to create a European governance structure on AI in the form of a framework for cooperation of national competent authorities in order to avoid fragmentation of responsibilities, increase capacity in the Member States, and make sure that Europe equips itself progressively with the capacity needed for testing and certification of AI-enabled products and services.

Finally, at the end of the White Paper, the Commission launched a broad consultation of Member States civil society, industry and academics, of concrete proposals for a European approach to AI. The consultation closed on 19 May 2020. It will be fascinating to see the results of this dialogue in future legislative proposals.

DATA GOVERNANCE

It has been found that worldwide, between 2013 and 2015, we have produced more data than in all of human history up to that point. Today most of our daily activities (mainly online: internet searches, email, e-commerce, social networks, Skype but also instant messaging services such as WhatsApp), create data, which can be collected, analysed and monetized. Every day, we generate 3 quintillion bytes of data, an 18-digit number.

The ever-increasing amount of personal data is accompanied by an increase of their value in social, political and economic terms. In some sectors, especially in the online environment, personal data has become *de facto* the currency of exchange for online content. The data ecosystem is vast and complex and composed of an interconnected network of different actors who play across different levels. In this ecosystem, a business model based on the exploitation of data has been established. In this business model we can find excellent names - Google, Facebook, partly Amazon (which in addition to being the most important operator of e-commerce, is one of the most important cloud providers) and, together with them, a dense network which lives on data: data brokers, companies specializing in digital advertising, telecommunication companies.

In a recent report on the "Giants of surveillance", Amnesty puts under scrutiny what it defines as a "*business system based on surveillance*" in which individuals are constantly monitored in their virtual life and also in real life (for instance through voice assistants, that open the chapter of the internet of things).

It is no coincidence that this surveillance-based business system has had its breeding ground in the United States - where big tech companies have their headquarters - traditionally inclined to a soft / liberal approach on privacy issues.

On the basis of data protection, it can well be appreciated the profound difference in sensitivity between the "new" and the "old continent"

where, after a long gestation, the GDPR (2016/679) was born.

The EU General Data Protection Regulation (GDPR), which entered into force in May 2018, represents a global reference for data protection and privacy regulation. To wit:

“Shield” territorial scope: GDPR applies to all organizations located within the EU and also to those outside if they offer services or monitor the behaviour of people in the EU.

Objective scope: the EU Regulation defines personal data in general as *"any information relating to an identified or identifiable natural person."* The definition is deliberately very broad: and as a result, within the concept of personal data fall both *pseudonymised data*, which can be attributed to an individual through the use of additional information and *inferred data*, provided that they are linked to unique identifiers or are otherwise attributable to an identifiable natural person.

Other key principles of the GDPR are that of **"transparency"** and **"purpose limitation"**, which provide that companies that collect and process personal data must be clear with users about the terms and purposes of the processing.

The GDPR also sets a high standard for **consent** - informed, specific, free. When the processing has multiple purposes, consent should be given for all of them. Moreover, the GDPR philosophy revolves around the concept of accountability, a double track principle.

The GDPR foresees that the controllers put in place adequate and effective measures to

guarantee the security of the data but does not specify which kind must be adopted: the controller is free in deciding the most appropriate measures according to the type of processing, and its purposes for the use of and nature of the data.

The GDPR puts a huge emphasis on the **violation of privacy issues**, which can negatively impact controllers in the public and private sectors, both in economic terms and, above all, in terms of reputation. Therefore, it is necessary to minimize risks, build and maintain a good reputation and guarantee the trust of citizens and consumers.

“Data breach” means the security breach that involves the destruction, loss, modification, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed.

According to the GDPR, notification of any data breaches must be made without unjustified delay and, where possible, within 72 hours, from the moment in which the violation has come to light and any delay must have good cause.

The minimum content of the notification is outlined in article 33 of the GDPR, the competent European Data Protection Authority will provide online forms requesting mandatory information. This documentation allows the Control Authority to verify compliance with the requirements.

When the violation of personal data presents a high risk for the rights and freedoms of natural persons, the data controller notifies the data subject of the violation without undue delay.

The communication to the person concerned, shall describe in simple and clear language the nature of the violation. This communication is not required if the data controller has implemented the appropriate technical and organizational protection measures and these measures were applied to the personal data subject to the violation, in particular those intended to make personal data incomprehensible to any-

one who is not authorized to access it, such as through methods of encryption.

About the Authors:

Federico Gabbricci is Researcher at The Thinking Watermill Society, and Deborah Bolco is Partner of Pavia e Ansaldo Law Firm.







Short Overview Latin America

The following overview of Latin American frameworks was collected in part from insights contributed by hosts of the 2019 edition of the WLS summit, and research by the WLS global team. The full digital publication of global insights and highlights from the 2019 summit are to be published at www.worldlegalsummit.org later this year (2020).

It is well known that when it comes to the adoption of new technologies Latin American countries are leading the way in numerous

domains. Many emerging technologies, particularly blockchain and identity solutions, have profound implications for the security of human rights and individual autonomy toward economic and social inclusion. Many Latin American countries face issues of government corruption and large scale violations of human rights. It is possible that much of the technological progress some of these nations are experiencing could be a social response to some of these issues, as a mechanism of creating improved access to

justice and economic inclusion.

Much of the progress of new technology adoption across Latin America could be due

in part to the relatively “blank slate” many of these countries have when it comes to regulatory frameworks for governing these technologies. On the same token, developing nations, including those in Latin America could progress these frameworks quicker than other jurisdictions with more mature legal structures due to the lack of complex legacy infrastructure.

There are promising indications that several Latin American countries could lead the way in posturing possible regulatory solutions which could merit similar applications in other jurisdictions.

Here we will summarize those that were discussed at the 2019 World Legal Summit (#WLS2019): identity and decentralized systems, AI and autonomous systems, and personal data governance.

Identity and Decentralized Systems

The concepts of identity and social inclusion are driving much of the progress Latin American countries are experiencing with digital identities and decentralized technologies. For example, expert panelists involved in the 2019 WLS Summit in Argentina indicated that the International Human Rights Treaties was one of the, if not the most, important element driving the development of the regulatory frameworks for technology that facilitates the management of personal identities.

Most Latin American nations now use a form of eID system with rapidly growing digital infra-

structures for the governance and management of these solutions. The most widely used e-credential system currently used across [Latin America is the 2D barcode card](#), which is a card encrypted via a 2D barcode. As an illustration of this progress, it is worth noting that [according to some](#), Latin America is becoming a world leader in the biometric market with increased investment by governments toward security spending, deployment of facial recognition technologies, and applications toward cyber-crime prevention.

The concept of Self Sovereign Identity (SSI) is taking hold in Latin American countries too, whereas it is a mere philosophical concept in most developed nations. Brazil, Argentina, and Mexico are for example supporting the adoption of decentralized digital identity systems, predominantly based in blockchain infrastructure. In addition, those same countries, along with Venezuela and Chile, have widely accepted the use of cryptocurrencies in retail outlets and market places. Though, it is worth noting that much of that use sits outside of government regulation where regulatory frameworks simply don't yet exist, and to that end several other Latin American countries, including Ecuador and Bolivia [have banned the use](#) of these digital currencies.

AI and Autonomous Systems

According to the Global Talent Competitiveness Index (GTCI), produced by Google and other partners, [Latin America is well positioned](#) to become a leader in global AI talent. This has to do in part with many of these nations scoring high on AI preparedness indexes, with 15 of the 100 top nations listed in the GTCI report being Latin American countries. Again, the nations

leading the way are Mexico and Brazil, along with Uruguay and Chile. Much of the driver of this AI adoption is due to indications that these technologies could greatly improve Latin American economies. For example, [some models estimate](#) that the compound annual growth rate (CAGR) of the Brazilian GDP would increase over 7% per year up to 2030 when the maximum benefits of AI are considered.

Part of these developments are due to large scale government investment into the research and development of AI, with [Mexico leading the way in 2018](#) as the first Latin American country to construct a national AI Strategy.

However, similar to many other regions worldwide, these investments are in large part dedicated to supporting the assurance of the [country holding a place in the global "race to win AI"](#) in terms of the development and research of these technologies. This is an indication that attention to the regulation and development of sustainable legal infrastructures to manage the adoption and impact of these technologies is perhaps lacking or poorly attended to. As a statement to this, Omar Costilla-Reyes, an MIT postdoctoral fellow and leader of AI ethics in Latin America, [has said](#), “Latin America needs to be an ethics-first AI continent to guarantee that the technology will be developed and deployed for social benefit ... such as [prevention of] the use of AI deepfakes to spread misinformation”.

Personal Data Governance

There is a growing emphasis on the importance of the EU's General Data Protection (GDPR) for nations worldwide, in terms of the

building of similar models. Although many Latin American countries had data protection regulations and policies in place prior to the enactment of the GDPR, it has still had much impact in shaping the current regulatory landscape. Latin American countries in particular are drawing on learnings from the GDPR and many countries are now in the process of constructing equivalent regulatory frameworks. Brazil has led the way with its development of the [General Data Protection Law](#) (Lei Geral de Proteção de Dados Pessoais, or LGPD), that applies to organizations managing or processing citizens personal data. Several other countries across the Latin world too have recently passed or are in the process of amending similar frameworks. Here is a sample list:

- Mexico: Federal Law for [Personal Data Protection Possessed by Private Persons](#) (DPL)
- Columbia: [Law 1581](#) that manages the processing of personal data and employers management of their employees data
- Chile: [Personal Data Protection Law](#)
- Argentina: [Personal Data protection Law No. 25.326](#)

One of the largest issues still remaining for the protection and stable governance of personal data across Latin American, is the incongruity of existing frameworks. Largely, these frameworks still exist in a federated legal landscape, where even within one nation there are regional or state specific bodies of laws to govern this space. While this is not a problem unique to Latin America, there are pressing issues with possible corruption and data mishandling that are amplified in these regions, which is creating an increased tension in demands for better regulation.

Brazilian Legal Framework in Connection with the World Legal Summit

By Paula Figueiredo, Lawyer, Professor, Speaker and Mentor of Founder Institute, and WLS Ambassador for South America

The digital transformation experienced in all areas of human knowledge and relations presents itself to the legal world with the demand for a transversal approach. This approach needs to be considered in the making of regulations and public policies by countries and states, the ruling of complex and not previously known situations, and the regulation of private relations and human rights under the new, rapidly changing, global technological and innovation landscape.

As a mechanism elected to enable life in society, the law must also support technological innovation in order to promote the growth and evolution of society, and must do so in a way that is not at odds with the well being of that society. The law's ability to support this evolution is critical to bringing humanity through the technological "teenager hood" it is currently undergoing in a way that serves society's best interest.



The main question to be answered is “where do we want this transformation to take us”? In addition to promoting the rights and interests of individuals, we need to determine the intended benefits and goals of the digital transformation and technology revolution.

Legal professionals may be, in this scenario, invited to consider attempting to control not yet known scenarios, whether efforts could be shifted toward the exploration of new legal avenues for the sustainable development of these technologies.

Addressing the challenges with this train of thought was the purpose that brought law and technology professionals from diverse backgrounds together across the world during the World Legal Summit on August 1st, 2019. The purpose was to discuss and propose how to address three subjects in particular: (i) digital identity; (ii) data protection and (iii) autonomous machines' regulation. The results of this work will be published in the digital publication to be released on the WLS website later this year, with some of the perspectives and insights presented in the articles included in this magazine.

To provide our readers with the context for Brazilian progress in regulation for each of those three technology domains, it is important to mention the regulation already published and/or the bills under discussion, as follows:

Digital Identity

The Brazilian Public Key Infrastructure (ICP-Brazil) was created in August 24th, 2001. Put simply, it allows natural and legal persons to take action in a digital environment, in particular regarding digital signatures and transactions. It came into force through the Provisional Measure number 2.220-2, enacted by the Executive Power. It is a system centralized by the ITI - Instituto Nacional de Tecnologia da Informação (National Institute of Informa-

tion Technology), a public and federal body that serves as the Central Certification Authority.

On the 18th year of the systems' enactment, the ITI stated that over eight million digital certificates were active, with significant growth in recent years. Law professionals across the country use digital identities regularly, as the Brazilian Electronic Judicial System requires use of this system for petitioning and procedural acts. In addition, the digital signature is needed for companies and corporations' regular activities, for example those activities related to the Brazilian fiscal system. With a population of about 209 million inhabitants, the system is not yet massively adopted: it is a paid system, with technological requirements for its access and operation. More cost effective and user friendly solutions could provide increased adoption of these systems. Wider adoption could also be seen as a result of the digitalization of a growing number of procedures and document use (as per public registries before notary public offices), a transformation which has been expedited due to the global Coronavirus pandemic. Further, the emergence of new technologies and improved systems of security are aiding the increased adoption of digital systems. Public policies managing the broader application of digital identities will also add to the Brazilian and global scale of these technologies.

Personal Data Protection

The Brazilian Law on Personal Data Protection (LGPD) was published on August 14th, 2018. The LGPD was set to be enacted eighteen months after its publication, though this plan was modified and it was not enacted until two

years after its publication. Two bills (one in the Senate, one in the Chamber of Deputies) have recently been proposed that aim to postpone the enactment of the LGPD even further. A Provisional Measure (959/2020) enacted by the Executive Power has superseded the ongoing legislative discussions, and include now an expected release date of May, 2021 for the data protection law. There are factors that could postpone the release of the LGPD even further than the currently anticipated date in 2021. For instance, the Provisional Measure has to be confirmed by the Congress to be converted into law. In addition, given that the proposal originated in the Senate and has the force of presidential sanction it may require further review, which could set the date back further.

The Brazilian Personal Data Protection Law is substantively based on many of the same provisions as the GDPR (General Data Protection Regulation - European Union). However, there are other aspects that differ and are subject to intense review as society prepares to comply with the regulation. The Data Protection National Authority (ANPD) members are yet to be nominated, however once in place this committee will be responsible for the regulation of the important technical aspects of the LGPD. The bill has undergone a turbulent beginning, having been under discussion for about a decade prior to its publication, and now with several Brazilian legal instruments involved, such as the Constitution, the Consumer Act, The Internet Law, the telecommunications regulation and more.

Furthermore, rising awareness in the market regarding the need for data compliance regulation is leading to increased measures being

taken to address these issues within companies and corporations as a first line of enforcement. A significant part of these discussions is Brazil's LGPD, which will be in force soon and will put Brazil in alignment with worldwide efforts to secure measures for personal data protection.

Artificial Intelligence

Presented in 2019 in the Senate, bill n.

5.051/19 is the pioneer proposal to address the regulation of Artificial Intelligence in Brazil.

As the regulation of AI is extraordinarily complex, further and wider discussion of the bill will be necessary. Given the concepts and implications of the bill, and its character as a general nationwide law, there are several challenges that lawmakers and legal professionals must account for and consider before its enactment. For example, any general AI regulation would need congruity with the Data Protection Law. In addition, it would need to address the several issues already raised with liability concerns, machine bias, algorithmic transparency and audit-ability. In fact, the regulation of AI and autonomous machines are among the greatest challenges faced by law professionals today across the world.

Could regulating efforts impact technological development? Is it even possible to regulate AI in its most extreme form? Is human authority at risk? These are issues that transgress human physical and political borders.

Collaborative efforts amongst legal professionals across jurisdictions is critical. In fact, the unfolding thesis surrounding these technologies is an intersection of several domains of knowledge, comprising computation and programming experts, data and data processing

scientists, product professionals and many others.

In Brazil, the first edition of the World Legal Summit also covered the National Bill for Startups' Incentive, which considers businesses and their models an important conduit for innovation and the progression of technology. The complementary bill project (146/2019) is currently in analysis at the Chamber of Deputies and the Executive Power's Public Consult which is preceded by a working group covering four main aspects: (i) investments; (ii) economic labor relations; (iii) public bidding (iv) market and environment aimed to reduce bureaucracy, increase incentives and provide the conditions for the launch and growth of these companies.

The transformative progress of technological innovation is impressive when considered against the amount of resources, time and effort it would take just a few decades ago to obtain similar results, especially when considering traditional economic models. Given this progress, one has to ask whether enabling access to technology and knowledge for its use is a fundamental human right? If so, how might we ensure this access and its sustainability at a global scale? Given technologies current capabilities, one also has to ask why humanity still faces so many issues? The World Legal Summit community is designed to answer many of these questions, and invites your thoughts and suggestions in the 2021 edition.

We would like to thank each and every participant who took part in the discussions held across Brazil during the 2019 World Legal Summit in Belo Horizonte and Minas Gerais.

In addition, we would like to recognize the Committee for Law for Startups of the Brazilian Bar Association, the Minas Gerais Session staff who were responsible for the event and organizing our sessions, and finally to Aileen Schultz, whose vision and resiliency made this worldwide effort possible, and who introduced the following words to my communications:

*Yours in legal transformation,
Paula Figueiredo,
World Legal Summit Ambassador for Latin America*

About the Author

Paula Figueiredo is Lawyer, Founder of www.thelegals.law (Advisory Law for Startups), www.figueiredo.law (Advisory Business Law), Legal Strategy and www.modacad.-com.br, World Legal Summit Ambassador for Latin America, Founder and President of the Committee for Law for Startups of the Brazilian Bar Association - Minas Gerais Session, member of the Committee for Law for Startups of the Brazilian Bar Association - Federal Council, Coordinator of the post-graduation course on Law, Innovation and Technology of the Superior School of Law - Brazilian Bar Association, Minas Gerais Session; Professor; Speaker; Mentor of Founder Institute (2018 and 2019/1 - Belo Horizonte Session) and many Startup acceleration programs. Mentor and Member of She's The Boss, Member of She's Tech, Elas in Tech and Women in Blockchain Brazil groups, for women entrepreneurship and presence in technology, as well as gender balance.





North America

By Aileen Schultz, Founder & President World Legal Summit, Senior Manager Labs Programs at Thomson Reuters.

The United States and Canada may be considered “ahead of the curve” when it comes to the adoption of some new technologies and their related systems, for example leadership in AI research and skill development. However, they are behind the curve with regard to other technological systems like blockchain enabled economies or digital

identity infrastructures. While many of the countries leading in these domains are leading at the expense of mature legal and regulatory frameworks, North America’s lack of adoption is arguably due to the lack of necessary legal frameworks supporting widespread use and implementation of these technologies.

Admittedly, much of the recent incentive placed on prioritizing sound regulatory systems in North America, likely comes from the many lessons learned from recent blunders within Big Tech. For example, monstrous data breaches and rogue autonomous machines have resulted primarily from the negligence of tech giants headquartered in the United States. Whether due to these recent blunders, or simply because of market incentives, Canada and the United States have significantly improved their technology governance frameworks in recent years. This is particularly true in key domains such as: identity and decentralized systems, AI and autonomous systems, and personal data governance.

I. IDENTITY AND DECENTRALIZED SYSTEMS

With [over 100 countries](#) now making use of digital passports or electronic identification (eID) programs, Canada and the United States are certainly late to the party. Nonetheless they can still benefit from the many use cases now available. Given North America's relatively few issues stemming from poor identity infrastructure, such as voter fraud or mass numbers of its populations that are without any legal form of identity, it is not surprising that these countries are only now considering the need for new frameworks.

It is surprising though that the adoption of decentralized technology infrastructures, such as the widespread acceptance of blockchain-based crypto currencies, has not gained traction in North America, considering that Ethereum and Bitcoin (two of the world's most popular blockchains) originated in Canada and the United States respectively. Whether this is due to the inherently “non-

jurisdictional” quality of these technologies or the low demand for alternative economies is unclear.

Canada: Digital Identity

There are indications that Canada could be steps closer to a national eID program as early as this year (2020). Citizens are demanding that the Canadian government invest more in the development of these frameworks, with [a 2017 survey](#) indicating that 70% of Canadians want to see the government work with the private sector to implement digital IDs. Industry associations like the Canadian Bankers Association, which have a pulse on consumer needs, are also [heavily advocating](#) for such a system in Canada. Furthermore, organizations are making headway in the development of a national digital identity infrastructure for Canadians. For example, the Digital Identification and Authentication Council of Canada (DIACC) is a non-profit coalition of industry leaders and organizations tailored to the promotion of a digital ID infrastructure for Canada. Its primary initiative, the “DIACC [Trust Framework Expert Committee \(TFEC\)](#)” is anticipated to be activated by July of this year (2020), along with [possible other industry frameworks](#).

According to the DIACC [a digital identity trust framework is](#):

- A set of rules and tools designed to help businesses and governments to develop tools and services that enable information to be verified regarding a specific transaction or particular set of transactions.
- Comprised of industry standards and best practices that define the processes to be followed to verify information about a person or a legal entity.

- Will help solutions to seamlessly work - or interoperate -“ together by establishing a baseline of requirements of public and private sector services.

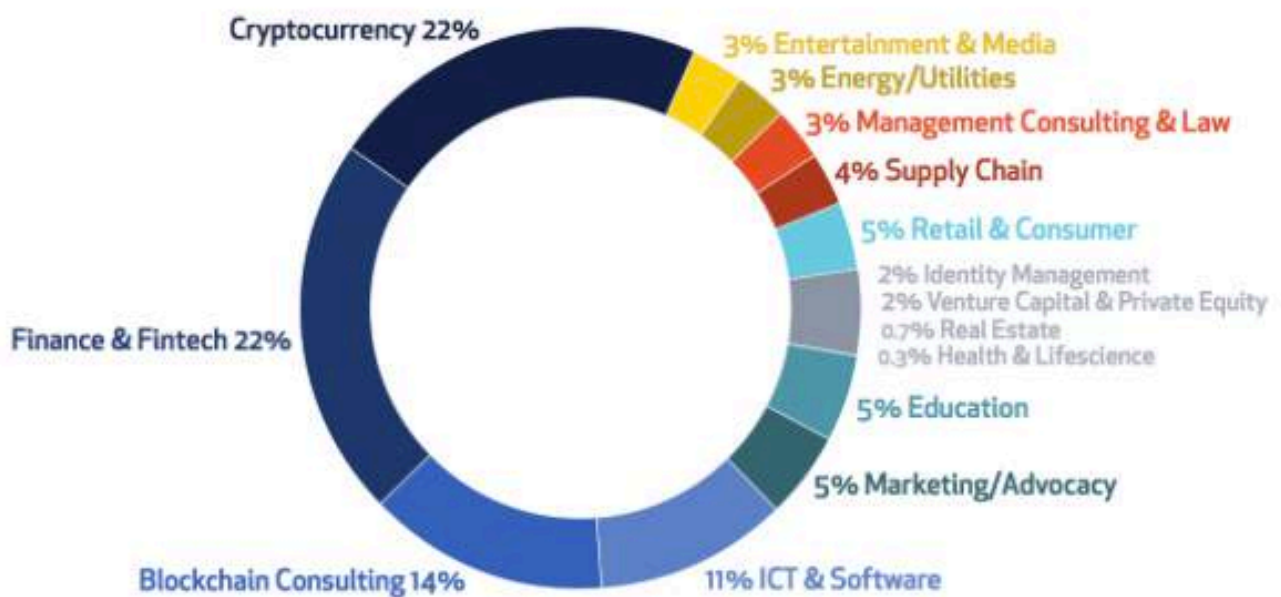
Such developments have led to statements that Canada is in a good position to become a leader of digital identity programs. Such a statement is perhaps a far cry, considering the comparative maturity of such systems in several other countries already. However, there is indication that Canada could be in a position to begin early considerations of a Self Sovereign Identity (SSI) framework where identity systems could begin to become decentralized, depending less and less on centralized institutions as they do currently. For example, as [stated by Franklin Garrigues](#), VP Digital Channels for TD Bank “Canada is moving forward with several initiatives to make it possible for customers to share their identification data held by one organization with another...For example, with consent, a bank

might access a customer’s driver’s license directly with the license bureau”. In order that this might become a true SSI system, Canada needs to consider what it might look like for organizations to access this data by going directly to the citizens instead of intermediary organizations like the license bureau”.

Canada: Blockchain and Decentralized Technologies

While the concept of blockchain technology and resultant decentralized systems are not altogether new conversations in Canada, their actual application has been limited. This is largely to do with the current regulatory challenges these technologies pose - a problem faced by many jurisdictions worldwide. However, there has been a recent upsurge in blockchain application across nearly every industry, which has put increased pressure on regulatory bodies and lawmakers to build the necessary legal infrastructure for continued growth in technology development and adop-

Figure 4: Canadian Blockchain Ecosystem, Companies per Sector



Source: ICTC

tion. The Information and Communications Technology Council (ICTC) recently [issued a whitepaper](#) detailing the Canadian landscape for blockchain adoption. True of just about every jurisdiction looking at these technologies, the banking and finance sectors are by far the most mature in terms of technology use and the development of governance frameworks.

However, something interesting to note is the general acceptance of the merits of these technologies as well as their application in the government. For example, with the Canadian Border Services Agency (CBSA) [piloting a use case](#) for improving data quality and to facilitate the more transparent shipment of goods.

In spite of the rising number of Canadian use cases across industries for these technologies, there is much work to do in terms of ensuring their sustainability with sound legal and regulatory frameworks. By far the most work in the [development of these legal frameworks](#) has been done with regard to digital currencies, particularly crypto currencies, however these currencies are still not recognized as legal tender. In terms of the vast opportunities for infrastructural applications of decentralized technologies, much work needs to be done to ensure the use of data, identity management, and governance protocols for these technologies are in keeping with current sentiment around privacy protection, institutional access, and trusted control.

USA: Digital Identity

Although the United States Department of Defense has had a fairly robust eID system in place for some time now, the military Com-

mon Access Card (CAC), wider adoption has not yet caught hold. The National Institute of Standards and Technology (NIST) are however making dedicated efforts to speed up that trend. The Obama administration put in place in 2011 a National Strategy for Trusted Identities in Cyberspace, which the NIST in collaboration with the U.S. Department of Commerce has been actively working toward program implementation for.

In large part the setbacks with technology adoption are to do with concerns associated with the technology itself, rather than having the appropriate regulatory framework for governing these systems. In terms of taking the progress of the government's use of these technologies and applying learnings to the private sector and use within the broader citizen populations, the transferring of government ID security measures has been raised as a major concern. In addition there are challenges around the approach taken to both the development of these technologies and the laws made surrounding their use, since currently many states have their own state-specific identity systems, complete with unique state issued ID cards.

USA: Blockchain and Decentralized Technologies

Like with Canada and the global blockchain industry, the United States has put much of their regulatory attention at the administrative and agency level (e.g. the Securities and Exchange Commission "SEC" and the Federal Trade Commission "FTC"), with a primary focus on crypto currencies and the entities controlling them. In addition, given the unrelenting growth of crypto currency use and adop-

tion in nefarious underground cyber worlds (a.k.a the “darknet”), the USA has felt the pressure of needing standards and modes of governance to respond to these bad actors (rightly so).

The U.S. government [has launched the Cryptocurrency Intelligence Program](#) as a response, implicating new tax reporting and regulatory requirements. For example, taxpayers are now required to report any income obtained via virtual currency use.

Similar to the development of digital identity legislation, much of the regulation surrounding blockchain technologies has [occurred at the state level](#). With some states encouraging the application of these technologies, including crypto currencies, in hopes of spurring investment and development in these areas. Particular [progress has been made in Arizona](#), where a regulatory sandbox has been substantiated to encourage the development of new blockchain applications, and the necessary regulatory frameworks for wider adoption. Though, several other states (at least 10) have made statements of warning about investing in crypto currencies.

Given that one of the (if not *the one*) best known infrastructural applications of blockchain technology was born from a partnership between two U.S. headquartered companies, it is probable that the U.S. could lead in broader governance frameworks for the use of decentralized technologies. The [IBM Maersk use case](#) for shipping and global trade, announced in 2018, is a global collaboration between more than 90 organizations including over 20 port and terminal opera-

tors worldwide. Lessons learned from this use case could provide the foundations for coherent and globally salient legal frameworks.

II. AI AND AUTONOMOUS SYSTEMS

When it comes to emerging technologies and global systems, AI is perhaps the most infamous. Nations are competing to win it by promoting multibillion dollar investments in the research and development of these technologies, the attraction of talent, and fortunately in some cases the progress of regulatory and ethical guidelines. AI technologies have witnessed an upsurge in development due to the vast amounts of data we now have available like never before. North American companies, particularly tech giants and social media goliaths in the U.S. have witnessed an advantage given their access to global user data that was beginning to be acquired well before our knowledge of just how valuable that data would inevitably become. With all this attention to the development of the technologies, sound AI governance is lack-luster to say the least.

As a result the autonomous systems made possible by these technologies too are lacking in sound governance frameworks. Both government and private sector organizations are making efforts to define these standards in the development of these systems, but to date much of these developments sit at the industry level and lack legal ramifications for misaction. Smart contracts, though not dependent upon AI for execution, are nonetheless greatly enhanced by AI technologies. And as algorithms themselves, smart contracts can in turn greatly increase the scalability and application of AI technologies.

As self-executing contracts that are effectively traditional contracts turned into computer code, these algorithms (“smart contracts”) together with developments in AI are paving the way to a vastly autonomous future across every industry; a future that is equally lacking in sufficient regulatory frameworks across North America.

Canada: AI

The Canadian Chamber of Commerce published a whitepaper titled “Automation Not Domination: Legal and Regulatory Frameworks for AI” in 2019, just about one year ago as of the writing of this article. The title shed light on the general global “fear of robots”, a sentiment not unique to Canadian organizations. A sentiment that the Government of Canada responded to in 2019 with a [Directive on Automated Decision-Making](#). Yet another title that drives home where the real concerns about AI sit, with decision making that is outside of human control.

This Directive however is focused on the government's use of these technologies, and does not yet apply to the private sector, leaving a large chasm between companies developing and applying these technologies and their governance. As set out in section 4, the objectives and expected results of the Directive are primarily focused on the sound use of data by the government, and are as follows:

4.2.1 Decisions made by federal government departments are data-driven, responsible, and complies with procedural fairness and due process requirements.

4.2.2 Impacts of algorithms on administrative

decisions are assessed and negative outcomes are reduced, when encountered.

4.2.3 Data and information on the use of Automated Decision Systems in federal institutions are made available to the public, where appropriate.

Where legislation dealing with the private sector has come into play is with regard to anti-competition laws, and the possibility that companies with unparalleled amounts of data may be at an advantaged surplus in terms of AI development and as such this could interfere with currently respected anti-competition sentiment. Furthermore, Canada was the first country to launch a [federally funded national strategy for AI](#) managed by the Canadian Institute for Advanced Research. However, the strategy is meant to increase investment in the research and development of AI to encourage global leadership, and is not focused on the development of regulatory frameworks.

Canada and USA: Smart Contracts

The Canadian government has been relatively deliberate in its moves to [postpone the allowance of smart contract systems](#), until the technology is further developed and regulatory structures are matured. However, there is indication that the use of smart contracts and their legal viability is not too far off. Canadian courts, for example, have already determined that “click wrap” agreements (the “I agree” checkbox on websites) [are enforceable](#).

Similarly the [U.S. has not had a case](#) in which to set a precedent and does not have any current laws equipped to deal with cases involving the use or misuse of smart contracts.

However, there are some elements of the existing legal framework dealing with the writing and signing requirements of contracts that could transfer to the use of smart contracts. For example, in a sense smart contracts could be argued to be allowed under the current Uniform Commercial Code (UCC) that indicates that contracts do not necessarily need to be in writing. It could be inferred that this could mean that not every contract needs to be in natural language, and could for example be in machine readable language or “smart contract” form.

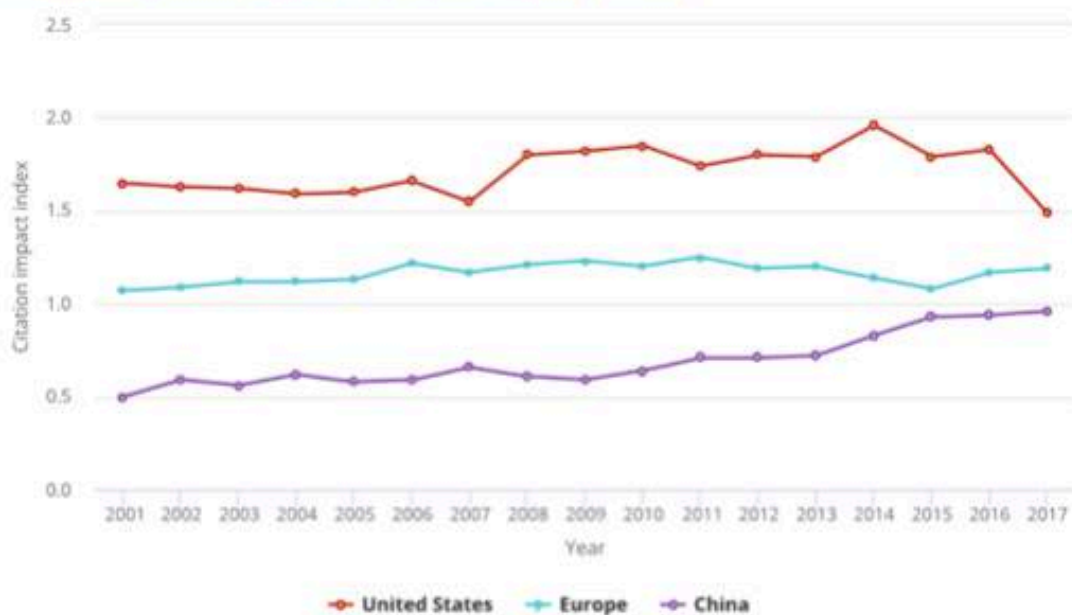
USA: AI

The U.S. is widely considered to be a leader in the development of Artificial Intelligence technologies, based on a [recent WIPO study](#) that indicates that USA based companies and Chinese based companies make the large majority of AI patents issued. In particular, IBM and Microsoft (U.S. companies) currently hold first and second place for the most amount of AI patent applications. In addition, the U.S. leads in scientific papers citations for AI research according to the National Scientific Board of the USA.

National Science Board | Science & Engineering Indicators | NSB-2020-5

FIGURE 6-16

Citation impact of AI scientific papers by selected region or country: 2001–17



AI = artificial intelligence.

Note(s)

The citation impact shows the degree of citing AI publications in a region or country relative to the world. An impact of 1.0 indicates that AI scientific publications are cited at the same frequency as all other regions. An impact of greater (less) than 1.00 indicates that the publications of a region/ country are cited more (less) than would be expected.

Source(s)

The 2018 AI Index Report. 2018. Artificial Intelligence Index.

Science and Engineering Indicators

Similar to Canada, when it comes to federal regulation and the formation of bills and regulations, much of the attention has been given to the regulation of the government itself.

While this is not of course a bad place to start, given the dire need for sound government use of AI, it does leave private industry to its own whim and possibly dangerous application of these technologies. Though it is worth noting that several states have made moves to legislate and provide regulatory action toward the governance of the private sector.

Furthermore, the National Defense Authorization Act for 2019 does seem to take considerations of AI to a deeper level than its Canadian counterpart the Directive on Automated Decision-Making. For [example, subsection \(g\) of the Department of Defense's activities](#) provides the following definition of AI:

In this section, the term “artificial intelligence” includes the following:

- (1) Any artificial system that performs tasks under varying and unpredictable circumstance without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
- (2) An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.
- (3) An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
- (4) A set of techniques, including machine learning, that is designed to approximate a cognitive task.
- (5) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

III. PERSONAL DATA GOVERNANCE

Cybersecurity and the management of Personally Identifiable Information (PII) has seen a global rise in attention from regulatory and law making bodies. In North America things have been slower than elsewhere, for example with Europe’s GDPR setting the stage for nearly every jurisdiction’s data privacy regimen to come worldwide. However, there are some groundbreaking technological developments in U.S. based academies, with for example the work of the MIT Media Lab and project Enigma: “a peer-to-peer network, enabling different parties to jointly store and run computations on data while keeping the data completely private.”

Canada

The most well known and important federal statute dealing with the management of personal data is the Personal Information Protection and Electronic Documents Act (PIPEDA). PIPEDA was passed in 2000 and fully in force by 2004, indicating that regulatory concerns around personal data management is not a new consideration in Canada.

In origin PIPEDA was enacted to protect consumers’ privacy while also enabling Canada’s businesses to compete in the global digital

market. However, [PIPEDA has federal jurisdiction only](#) over federally regulated organizations and at a provincial level only Alberta, British Columbia, and Quebec have adequately similar frameworks.

In addition to PIPEDA, overseen by the Privacy Commissioner of Canada (OPC), there are more specific statutes and guidelines dealing with for example specific industries or types of information. Some examples include:

- Nearly all jurisdictions across Canada have a legislative framework that acts to manage the use and protection of health information.
- Criminal charges can be laid against those that willfully intercept private communication or the functioning of a computer system.
- Canada's Anti-Spam Law (CASL) covers the installation of software or a computer program without consent, the use of the software or program to communicate with others, the sending of spam emails or the use of contact lists without consent to use, amongst other provisions.

With growing digital activity, Canadians are concerned about how their data will continue to be protected, with [71% indicating](#) that the protection of personally identifiable information will be one of the most salient challenges facing the country in the next decade. As such, similar to nearly every jurisdiction world-wide there is much work to be done to protect the privacy of citizens against the ever increasing nuances of data acquisition and usage capabilities.

USA

Some have wondered how it is that Facebook, Amazon, and a plethora of other Big Tech firms have been able to neglect so much with regard to generalized data protection of their users and customers. However, this is less surprising when it's realized that the U.S. is one of very few countries that does not actually have a general federal statute to address data protection and cyber security. While the U.S. has been heavily criticized for this apparent lack of protection, that is perhaps unfair. The U.S. does have hundreds [of laws at both the federal and state level](#) to protect personal data across a host of sub classifications, for example industry specific legislation. Furthermore, the Federal Trade Commission (FTC) does have broad abilities to enforce penalties to protect citizens against unfair or deceptive actions taken by use of their personal information on the backbone of the suite of existing privacy and protection legislation.

The hundreds of laws that do exist are mostly sector specific, for example the Driver's Privacy Protection Act (DPPA) that protects the privacy and personal information of consumers from misuse by state level Departments of Motor Vehicles, or the the Children's Online Privacy Protection Act (COPPA) that aids in protection at the federal level of children under the age of 13 from data collection online.

Though there are these sector specific examples of legislation governing the protection of Personally Identifiable Information (PII) there is demand for a more generalized data protection regulation, given the cross sector, cross jurisdictional, cross device, nature of data acquisition and management today. With the

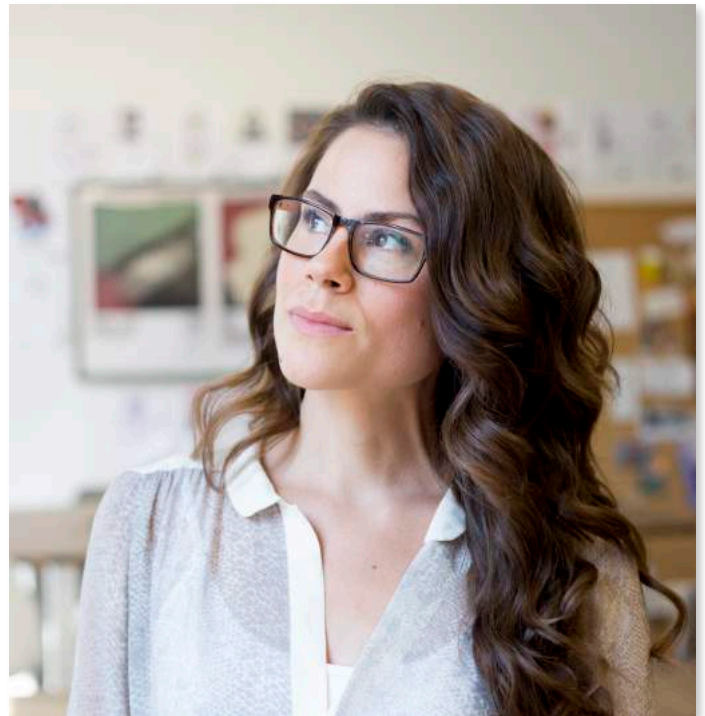
rise of IoT and increasing mechanisms for the misuse of data, there is a demand for a more accessible, transparent, and pragmatic approach to the protection of personal data in the U.S.

As a mechanism of responding to this demand, there is [a new Data Protection Act](#) which aims to substantiate a federal Data Protection Agency. These are efforts in line with the general global prioritization of efforts similar to that of Europe's General Data Protection Regulation. If successfully enacted, this agency would have authority to protect U.S. citizens across the country irrespective of sector or state specific legislation.

About the Author:

[Aileen Schultz](#) is a Toronto based award winning innovation strategist with a global footprint, and a passion for creating better systems for exponential change. She is particularly focused on effecting change at the cross sec-

tor between law and technology. She has a background in research, marketing, and digital strategy, having worked in the legal innovation industry for several years. (Founder/Creator Global Legal Hackathon, MIT, UofT, FastCase 50 Global Innovator)

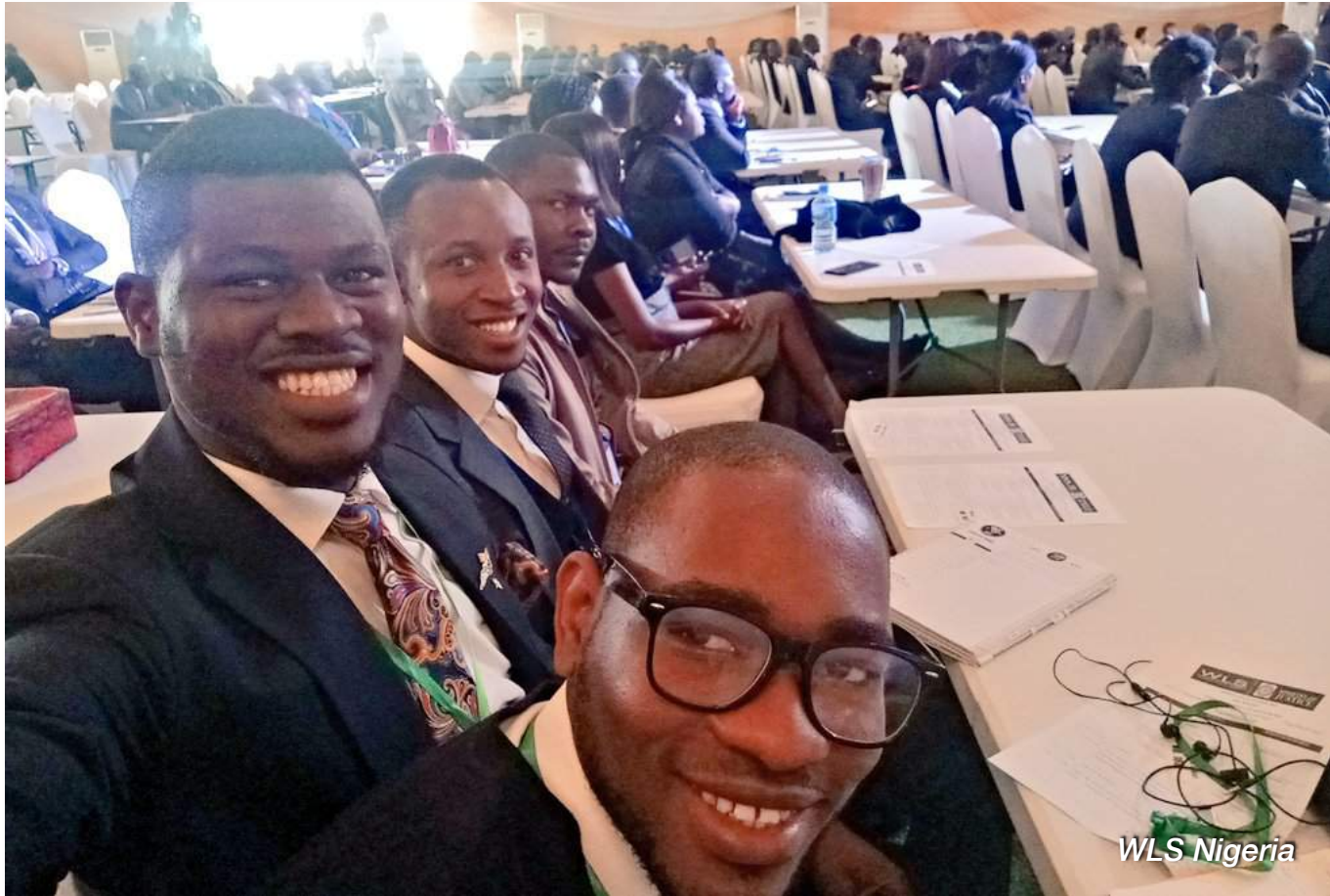


WLS IN ACTION





WLS Moscow



WLS Nigeria



World Legal Summit

Technology Themes

Section overview

Topics on Technology Governance

The World Legal Summit ecosystem consists of a community of diverse practitioners across the law and technology sectors. The following insights are shared by this community and are a selection of perspectives on key topics of technology driving the WLS initiative.

Surrounding our three “technology pillars” is a whole array of subtopics and considerations, such as what the future of governments and tech governance look like in a world driven by AI, or future possibilities for identity structures, and of course what the landscape for tech governance looks like on the other side of the pandemic.

This body of articles covers these topics along with a diverse set of author perspectives on these issues surrounding technology governance. These are not official statements of the WLS, but rather collectively an open invitation to join this community in engaging in this challenging dialogue. There are very few clear courses of action for many of these issues, however there is a massive community of experts in these domains and a growing community of invested interest in pursuing these conversations. It is through the ongoing discussion and dissemination of these diverse opinions and community insights that will allow us all to learn from and distill globally salient takeaways.

Renewing Multilateral Governance in the Age of AI

By Daniel Araya, Consultant, Advisor, CIGI Senior Fellow, and World Legal Summit Senior Partner



COVID-19 has proven to be a [very deadly contagion](#). In just a few short months, the scale and spread of the virus has been breathtaking. As [Fareed Zakaria observes](#), “We are in the early stages of what is going to become a series of cascading crises, reverberating throughout the world” Infecting [over five million people and killing close to four hun-](#)

[dred thousand worldwide as of June 2020](#), COVID-19 represents a massive global challenge. Nothing less than innovation, creativity and networking.

Responding to the current crisis has not been easy. As governments around the world struggle to manage the spread of the disease,

many are wondering what new tools are needed to moderate a probable economic depression. Even as central banks expand quantitative easing (QE) to stimulate the global economy, the impact of the pandemic on both employment and consumption now ensures an economic contraction that is both broad and deep.

The [consequences](#) of the current economic crisis remain difficult to forecast. What we do know is that the pandemic has exposed the fragility of the global supply chain system. In addition to this, the current crisis has also accelerated technological trends that were already beginning to reshape the geopolitical and regulatory landscape. Long before the pandemic, there was a growing need to rethink global institutions for a digital era.

COVID-19 is forcing governments to restructure their supply chains, but it is also reinforcing technological trends that had already begun prior to the pandemic. Data-driven advances in artificial intelligence (AI) and machine learning (ML) have begun reshaping the global economy. Fusing together the physical, digital, and biological worlds, the “datafication” of every aspect of human social, political, and economic activity is now driving new industries and new regulatory frameworks.

The Global Data Economy

As former BlackBerry Chairman and co-CEO [Jim Balsillie](#) explains, this data-driven revolution is not only remaking the terms of global trade, it is transforming the nature and distribution of power. In this new era of "[surveillance capitalism](#)", data has become the new oil. Unfortunately, the current multilateral

system was designed for an older era.

The world's economy is now increasingly structured around the critical importance of cross-border data flows. In fact, data flows now generate more economic value than traditional flows of traded goods. In 1976, 16% of the S&P 500 was made up of intangible assets (patents, trademarks and copyrights). Today it [is 90%](#). Intellectual property (IP) and the data it protects are the world's most important commercial and national security assets.

Even before the pandemic, the multilateral system overseen by the World Trade Organization (WTO) was already unravelling. Unlike the economic dynamics of the past, open markets are now driving market consolidation rather than competition. [Software is eating the world](#). And in this new era of [techno-nationalism](#), winners take most as countries and companies strategically leverage the network effects of technology platforms to reshape a collapsing Bretton Woods order.

What we are now seeing is a struggle for a new global order. This [includes a likely economic decoupling between the US and China](#). Building on rapid technological development across East Asia, China's economic and political influence has expanded dramatically. And so has the Chinese government's geopolitical ambitions. The global balance of power is shifting as [Asia once again becomes the center of world trade](#).

Moving Away from Hegemonic Structures
Since the close of World War II, our global order has largely been overseen by a siloed and nationalistic global power built on fossil fuels.

Even before the pandemic it was clear that the current multilateral system was under strain. The resurgence of nationalist agendas around the world and the dwindling capacity of the current system to play a meaningful role in a declining American-led order, signal a massive geopolitical shift.

In this new century, the days of unipolar hegemony are coming to an end. We are now in the midst of a digital arms race in which competition between software stacks and digital business models is remaking the global landscape.

As frictions around technology transfer and a contest for global technology standard-setting increase, so does the potential for global conflict.

Indeed, even as populism grips many Western countries, free trade deals have begun accelerating across Asia as the region becomes the epicenter of [global manufacturing](#). Asia's Regional Comprehensive Economic Partnership (RCEP), for example, now represents the world's largest trading bloc. Building on six years of negotiations, RCEP joins the Association of Southeast Asian Nations (ASEAN) together with China, Japan, South Korea, Australia, and New Zealand.

In fact, the drive for binding international agreements like the Trans-Pacific Partnership (TPP) and the recent USMCA reflect a geopolitical struggle to remake the global economy around digital asset protection. Whereas the industrial economy was dominated by the production, trade, and consumption of tangible goods, the digital economy is built on the

production, collection, and protection of information. Beyond the raw resources and tangible goods of the Industrial Age, the global economy is now increasingly run by a system of IP-driven trade deals.

Renewing Multilateral Governance

The [law of comparative advantage](#) should drive global prosperity as countries produce more of the goods they have in abundance, in exchange for goods they lack. But the reality is that rent-generating assets and big data are now accelerating an economy structured around [digital landlords and digital serfs](#).

Even as states now begin [debating new rules for digital trade](#), governments in countries like [China](#), Russia, and Brazil have already begun to develop their own. China's rapid technological advances in particular have intensified geopolitical tensions.

The truth is that technological innovation has been undermining the global multilateral system for some time. Building on supply chain challenges which have now been exaggerated by the pandemic, the world's governments are now being forced to consider new institutions for managing the data economy. In response to this unprecedented confluence of events, a new global regulatory architecture is needed.

Towards a Digital Bretton Woods

Together, the platform economy, surveillance capitalism, and AI are features of an emerging global system that demands institutions to balance against increasingly entrenched power that is rooted in centralized nodes of influence. As [Rohinton P. Medhora and Taylor Owen](#) point out, digital technologies and the coron-

avirus are both manifestations of a hyper-globalized system that is simply under-managed. And this weakness in the multilateral order now threatens to deepen the world's economic, geopolitical, and technological cleavages.

Any new framework for governing this era will need to ensure that trade, cybersecurity, personal privacy, national sovereignty, economic access and a host of other concerns are resolved together, under a single multilateral umbrella.

At the same time, the provision of digital products and services, including cloud computing applications, the Internet of Things (IoT), smart cities, etc., simply cannot function if cross-border data flows are restricted.

Even as the fundamental dynamics of the current global governance framework begin to unravel, a new set of legal and regulatory structures is needed. Leaders and policymakers will increasingly need to confront the reality that a changing geopolitical map will mean formulating new multinational data-sharing agreements, new guidelines for interoperable digital systems, and new compacts for regulating cross-border payments data.

What we now need is new digital Bretton Woods order to manage against the potential collapse of the existing multilateral system. As Medhora and Owen suggests, this might include a [Digital Stability Board](#) (DSB) to shape global standards, regulations, and policies across the platform economy. Much as the postwar order, this new multilateral system will need to respond to the negative im-

plications of the digital revolution while recognizing the changing nature of global power.

Any new multilateral system will need to appreciate the changing nature of a post-Western world. Any renewal of multilateral governance will mean integrating economic giants like China and India. Notwithstanding their rising geopolitical influence, both are being drawn further into multilateral rule-making. Indeed, even as [China builds "counter-hegemonic" institutions](#) that challenge traditional orders, both China and India must negotiate with the existing multilateral system.

But how long will this hold? Politically, legally, and financially, the current multilateral order is not structurally prepared for the changes now impacting the global economy. Nonetheless, change is upon us.

The key question confronting policymakers today is "How can actors within the current global order anticipate, collaborate, and resolve emergent challenges within the face of a waning multilateral system?"

About the Author

Dr. Daniel Araya is a consultant and advisor with a special interest in artificial intelligence, technology policy, and governance. He is Senior Partner with the World Legal Summit and Senior Fellow with the Centre for International Governance Innovation.



Product Liability and AI: Who's Really at Fault?

By Myron Mallia-Dare, Business and Technology Lawyer, Miller Thomson LLP, and Advisor to the World Legal Summit

Artificial intelligence (AI) systems are becoming ever-present in our society. We see Chatbots deployed to communicate with clients and autonomous vehicles (AVs) utilized to move products and people. The level of sophistication and autonomy of AI systems has progressed at an exponential rate and should continue to do so. This innovation, coupled with the rapid deployment of AI systems across in-

dustries, means that the risk and frequency of harm caused by AI systems will increase. Yet, as AI systems become more autonomous, identifying the cause of damage will become more complex.

Canada's current legal framework - as with many jurisdictions throughout the world - is not well-equipped to address the complexities

of establishing liability to losses resulting from the use or operation of an AI system. This uncertainty can stifle innovation and increase the risk and liability for those organizations looking to develop, commercialize, and utilize AI systems. Instead of waiting for the existing legal framework to catch up, organizations should evaluate their risk exposure under the legal framework in which they intend to develop or utilize AI systems - and take steps to reduce this risk. This article will discuss some strategies organizations can adopt to mitigate this risk. Although this article will focus on the Canadian legal landscape, the issues and strategies discussed will be relevant to many other jurisdictions.

Canada's Current Legal Landscape

Canada's current laws that apply to product liability claims are complicated. Legal concepts of contract, tort, and, in certain instances, consumer protection legislation may apply to the AI system.

Both federal and provincial laws may apply to the design, manufacture, and sale of products in Canada. Certain goods, such as hazardous products and automobiles and related products, face additional oversight. Each province has passed specific laws relating to the sale of goods and consumer protection requirements. These include the establishment of implied warranties under provincial statutes, such as the requirement that the goods be of merchantable quality. Except under certain circumstances, these laws and obligations will apply to the sale of products within the province. The basis for most product liability claims fall under Canadian tort principles. The three common causes of action arising from a defec-

tive product are based on: (i) negligent manufacture; (ii) negligent design; and (iii) failure to warn. Generally, a successful plaintiff must establish that: (i) the defendant owes a duty of care to the plaintiff and breached the requisite standard of care; and (ii) there was a defect with the product that caused the negligent act and the harm suffered.

As multiple parties are typically involved in the design, manufacture, sale, and utilization of a product, more than one party may be the subject of a claim. A party to a suit could be found liable for damages or injuries caused by a product depending on the duty they owe. Manufacturers, for example, have an overarching duty to manufacture a product that is reasonably safe and to inform relevant parties of risks associated with the use of the products they produce.

Existing tort law principles that apply to product liability claims are ill-equipped to address liability caused by AI systems. Identifying the "defect" in a malfunctioning product that utilizes AI will be challenging. These difficulties will compound with the deployment of more advanced AI systems in which the decision-making processes of the AI system is either unclear or unknown - such as with "black box" algorithms. Even if the defect is identified, proving a specific party's negligence within the supply chain of a product will be challenging to establish.

The shortcomings of the existing legal framework applied to AI is well illustrated in the context of AVs. AVs require numerous components, such as sensors and "traditional" mechanical parts, that provide inputs to the AI

system. The AI system then processes these inputs and makes decisions based on the data available. In an accident involving an AV, identifying the root cause or offending component could be problematic. AI systems autonomously make decisions based on all inputs it receives. Determining which component caused the AI system to malfunction - or if the malfunction was directly attributable to the AI system itself, would require a complete understanding of the AI system's decision-making process. Thus, establishing the cause of the harm or damage may be complicated, if not impossible.

Managing the Risk Through Contract

Even with the most stringent design and build requirements and safety protocols, it is inevitable that something will go wrong. The effects of these failures could be catastrophic to any party involved in the design, build, commercialization, or utilization of the AI system. This risk will become ever more apparent as products utilizing AI systems are deployed in the world. As these AI systems become ever more interconnected, defects or cybersecurity attacks may impact multiple, or worse, a whole network of products utilizing specific AI systems. Given the potential financial and reputational risk associated with the deployment of AI systems, it would be wise for parties to, as best as possible, negotiate and predefine each party's risk and liability before a loss occurs. This is critical when considering how existing legal principles are ill-equipped to address product liability claims relating to AI. Organizations involved in the development or sale of AI systems should review their contracts with both suppliers and customers to determine the scope of responsibilities and obligations as between them and to tailor such terms to the AI system

developed or sold. Developers may wish to contractually waive or limit their liability or require customers or suppliers to indemnify against certain liabilities that may otherwise fall on such organization. Unfortunately, there is no one size fits all approach to addressing this risk. Organizations will need to consider what laws and legal principles apply specifically to their AI system, including how this system is utilized. AI developers and users of AI systems should also review the terms of their insurance policies to confirm that they can rely on these policies and are adequately protected.

Conclusion

Advancements in AI will likely lead to a transfer of liability from the end-user to developers or suppliers of the products incorporating AI. To account for this shift in liability and to address the apparent inability of the existing legal framework to address product liability claims arising from complex AI systems, organizations involved in the development or sale of AI systems should carefully evaluate their exposure to liability claims to limit this risk contractually.

About the Author

Myron Mallia-Dare is a business and technology lawyer at Miller Thomson LLP in Toronto. His practice focuses primarily on domestic and international mergers and acquisitions, private equity, venture capital and corporate finance with significant experience in the technology sector. He regularly advises on complex technology transactions in the areas of artificial intelligence, FinTech, data management and blockchain. Myron routinely writes and speaks at various conferences and seminars on topics relating to emerging growth markets and the legal impacts of innovative technologies.



WLS Barcelona



WLS Madrid

A portrait of Alice Nawfal, a woman with long dark hair, smiling. She is wearing a light-colored top and small earrings. The background is a soft, out-of-focus grey.

Tech Governance:

The future of Digital Identity

By Alice Nawfal, Cofounder and COO of Notabene

In this digital age, building trust in online transactions is fundamental for the success of the global economy. Without adequate and cost-effective trust mechanisms, people and businesses may find it expensive to participate in digital transactions. Proper online identification and digital identity systems solve this. They are essential to enabling ac-

cess to digital services - whether financial, economic or social - and have been deemed as one of the primary GDP growth drivers over the next decade. A McKinsey study in 2019, “Digital identification: A key to inclusive growth”, estimates that countries implementing digital identity could unlock value equivalent to 3-13% of GDP by 2030. [1]

However, complexities abound in the design and implementation of digital identity systems. The amount of data that people share to “identify” themselves has grown exponentially, and that has given rise to many issues: How and where do receiving parties store this information?

With whom do they share it with? What systems are in place to stop data misuse - through data breaches or through the participating parties themselves? Can it be used for predatory or discriminatory practices against consumers? More broadly, how should digital identity systems balance collection of personally identifiable information with data protection? With what security measures should they be designed? What constitutes a “correct” set of attributes for identification - when there is no “one size fits all” definition of digital identity across industries or jurisdictions?

These are some of the questions that have made it difficult for regulators and industry groups to align on a unified governance framework for digital identity. There have been increasingly active attempts to address this by policy makers. A summary of their efforts is covered below. However, a more robust legal and regulatory framework will need to be introduced in the next 1-2 years for digital identity systems to be properly implemented for a truly trusted digital economy.

I. Defining digital identity - no one size fits all

Digital identity is a digital representation of a natural or legal person’s identity. Identity is a very complex topic, as the word itself encompasses many meanings and interpretations depending on the context in which it is used. In its

simplest form when used as a form of authentication to gain access to certain services, it is a set of attributes that uniquely define a person. Before the move to digital, traditional identity systems, often defined and run by national or local governments, consisted of a set of attributes that were static in nature. Digital identities, in contrast, can consist of not only unique identifying characteristics like digital signatures but also of all of the data associated with the person online, aka their digital footprint. This can include their financial transactions history, their social media networks, their shopping preferences, and their browsing history. This data is dynamic and constantly evolving. As such, digital identity looks more like a complex relational web [2] consisting of nodes (a transaction, a video post, a playlist) and connections between them (formulas that infer relationships, recognize patterns and predict behavior). Groups of them form clusters that are owned by specific services (Spotify account, e-gov website profile). Your digital identity is a collection of these clusters.

A person often displays only clusters or subwebs of that identity to gain access to a specific service online. Unlike traditional identity systems, these online attributes and clusters have mostly been defined and put in place by tech companies and businesses, often without proper oversight. Their users’ data, whether provided by the users or generated on their platform, also lives with them, stored as fragmented data silos. Users thus in many cases have little control over their own digital identities. This illustrates some of the complexity that exists with digital identity, and why legal frameworks and guidelines for digital identity systems are necessary to be instituted by governing bodies.

For the rest of this article, we take a narrower definition of online digital identity and hone down on “high assurance” digital identity. Assurance refers to the “level of confidence in the reliability and independence of a digital ID system and its components.” [3] High assurance is defined as meeting public and private sector’s standards for access to critical services, like opening a bank account or voting, and is often recognized by authorities for regulatory purposes.

II. Overview of governance and technical frameworks

While there exists no single digital identity framework, in recent years different standard-setting bodies and regulators have issued guidance or frameworks on this topic. It is expected that the standards they propose will be increasingly aligned. However, shortcomings of these guidelines remain on implementation effectiveness, definition / breadth of identity (many encompass only high assurance identity), and lagging behind evolving technology. Regulators and governing bodies need to address these shortcomings. Most importantly, they need to also integrate these guidelines into broader regulatory frameworks around data protection, consumer protection laws and digital rights. Without a more integrated approach, there is a high risk of failing to address the challenges listed below.

National or regional bodies

NIST Digital Identity Guidelines in the US ([NIST Special Publication 800-63-3](#)): The NIST guidelines outline the components of digital ID systems, breaking them down into two mandatory components and one optional:

- Identity proofing and enrolment: involves collecting, validating and verifying attestations to prove an identity, then establishing an account and binding the individual’s unique identity to these attestations.
- Authentication and Lifecycle Management: involves checking whether the person asserting the identity is indeed the one who was proofed (eg multi-factor authentication)
- Portability and interoperability mechanisms (optional) - relies on pre-existing identity credentials for access to new, unrelated services without conduct customer identification again.

The European Union’s electronic identification, authentication and trust services (eIDAS) regulation (EU No 910/2014): The EU’s eIDAS-Regulation was introduced in 2014 and has been fully in force since 1st July 2016. It introduces a single framework for the mutual recognition of digital identities among EU member states, with the goal of seamless cross-border recognition of digital identities.

It is part of an EU-wide integrated policy approach, reinforcing compliance with General Data Protection Regulation (GDPR) and privacy-by-design. eIDs under eIDAS allow for citizen control over identity data and selective disclosure.

Regulators hope to build on eIDAS to develop a “market-attractive, user-centric Digital Identity framework at EU level” [4]. This is big news, as it will pave the path for the adoption of decentralized or self-sovereign identity (SSI) systems in the EU (see opportunities

section below). The European Commission has already been experimenting with SSI, publicly announcing in March 2020 that it has built a SSI- eIDAS Bridge.

Global inter-governmental bodies

The Financial Action Task Force

(FATF) "Guidance on Digital Identity": As a global watchdog, FATF sets guidelines which it then expects local jurisdictions to implement within their regulatory frameworks. The guidance focuses on the use of digital ID systems strictly within financial systems, at regulated entities for customer onboarding and ongoing due diligence, as well as situations where regulated entities provide digital ID systems for customer identification/

verification to other regulated entities.

International standards organisations or industry-specific organisations

International standards bodies have been putting together technical standards for digital identification and authentication. The below table highlights a summary of these standards.

Identity-specific industry bodies like OpenID Foundation (OIDF) and Fast Identity Online (FIDO) Alliance support the development of technical specifications to build open and interoperable systems and industry certification programs, as well as the implementation of the above standards.

Organization	Standards
International Organization for Standardization (ISO)	<ul style="list-style-type: none"> • Identity proofing and enrolment of natural persons (ISO/IEC 29003:2018) • Entity authentication assurance framework (ISO/IEC 29115:2013 – under revision) • Application of Risk Management Guidelines (ISO 3100:2018) to identity-related risks • TC6861 Working Group 7, ISO is currently working on global standards for natural persons’ identification • Joint Technical Committee with International Electrotechnical Commission (IEC) for ID management
World Wide Web Consortium (W3C)	<ul style="list-style-type: none"> • Web Authentication browser/platform standard for MFA, using biometrics, mobile devices, and FIDO security keys • Standards for verified identity claims in decentralised identity systems (VCs)
International Telecommunications Union (ITU)	<ul style="list-style-type: none"> • Standards like ITU X.1277 (Universal Authentication Framework) and IT X.1278 (Client to authenticator protocol/Universal 2-factor framework) • Digital Identity Roadmap Guide in 2018 for aiding policy makers to design, develop, and implement National Digital Identity Frameworks
GSMA	<ul style="list-style-type: none"> • Technical standards applicable to mobile communications platforms, including standards for user identification and authentication with particular focus on decentralised identity, IoT, fraud detection and risk scoring

III. Considerations and issues with digital identity systems

While digital identity systems allow for more extensive identity proofing and robust ways for ongoing identity management, they come with their own risks:

Identity fraud, cybersecurity and data breaches:

Because both identity proofing and authentication happen over the internet, it provides ample opportunity for cyber attacks. At the identity proofing stage, fraud is easier forged en masse online than in-person, leading to higher incidences of identity theft. This can lead to “fake IDs” which bad actors use to facilitate illicit activities. Bad actors may impersonate individuals or create synthetic identities - persons who don't exist in the real world.

Meanwhile authentication risks come in the form of unauthorized access to legitimately issued digital identities, leading often to data breaches, loss or misuse of data. Bad actors employ multiple methods to gain access to individuals credentials, including phishing, man-in-the-middle attacks. They are getting increasingly sophisticated, with attacks to get access to multi-factor authentication methods (eg SIM attacks, theft of biometric authenticators).

Lack of standardization and interoperability:

There don't exist unified frameworks or technical standards for something as fundamental as digital identity. This is due to multiple reasons at play.

The first is complexity of what digital identity constitutes. This can differ across jurisdictions or industries, and presents a challenge to regulators or industry groups to come together and align on technical definitions and standards. Differences in incentives and goals being optimized for creates chasms among stakeholders. Financial regulators optimizing for reductions in financial crime through requiring increased personal data sharing can clash with the privacy industry, who are maximizing for consumer data protection. In a digital world, what constitutes identity attributes can also differ a lot from what it used to in a more traditional, physical sense before. Analysis of a consumer's recent financial behavior can be more reflective of their creditworthiness than their FICO score. These points make it difficult from a governance perspective.

Advances in technologies, and getting alignment across stakeholders (regulators, technical) takes time. What is important is educating stakeholders on the latest, but hoping they take into account that technology is not a panacea for solving some of the most fundamental and complex challenges of our time. It is fast paced, changing quick and a lot of it still untested en masse. Failures in technology for high assurance use cases can put people in vulnerability.

Data privacy and security:

While digital identity enables wider access to identification, solutions need to be balanced with improved privacy and security. Digital identity involves the collection and often processing of this data. The data en masse is now

vulnerable to data breaches or misuse, and with on-set of data privacy laws like GDPR and CCPA, identity service providers and regulated entities today need to determine how to instate strong data protection mechanisms. Businesses need not only fear regulators but increasingly realize that consumers expect it from them. Unless consumers feel that their data are protected, they will refrain from engaging with their services online.

Challenges amass in implementations of data protection mechanisms and determining the right way to provide access of data to consumers. For users, their personal data online is dispersed in segments across platforms and service providers. These providers have tied their revenue generation to the processing and usage of this data, and are not incentivized to give that up. It is impossible for users to gain back access to their old data - and even if they were, service providers like Facebook, Google, fintechs already have correlations about users beyond their raw data attributes. How do regulators govern the processed data - data they may not know exists and which may violate data protection mechanisms?

Decentralized identity solutions are being considered by regulators as an effective technological solution to help users gain more control over how their personal data is being shared.

Notes

[1] <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth>

[2] <https://techcrunch.com/2017/10/17/the-next-revolution-will-be-reclaiming-your-digital-identity/>

[3] <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf>

[4] <https://ec.europa.eu/digital-single-market/en/news/building-trusted-digital-identity-brochure>

About the Author

Alice Nawfal combines a business and policy background, and is passionate about bringing privacy-preserving technologies to market. She is the Cofounder and COO of Notabene, a compliance platform for digital asset businesses. Before Notabene, she was Project Co-Lead and COO of uPort, the decentralized identity platform anchored on Ethereum, where she led sales, marketing and operations. While at uPort, she ran successfully a digital identity pilot within the UK's FCA sandbox. Alice spent her earlier career as a Management Consultant at Bain & Company, and later as a Public Policy Consultant at the Economist Intelligence Unit. She has an MPA from the Harvard Kennedy School, an MBA from the Wharton School, and Math and Economics degrees from MIT.

About Notabene

Notabene is a compliance platform for financial service companies who provide or would like to provide digital asset services to their clients. Notabene helps them be compliant with new, global crypto regulations that come into effect this year.



Self-Sovereign Digital Identity

The Management of Identities and the Ability to Prove Who We Are

By Tatiana Revoredo - Blockchain & Cybersecurity: Advisor, Author, Strategist
* theglobalstg.com * [Liaison @ELONtech](mailto:Liaison@ELONtech) * Oxford Blockchain Fdn



The ability to prove who we are

One thing that is most critical for our society and economy to work effectively is a person's identity. Without means of identifying one another and our possessions, we would hardly be able to build great nations or create global markets [1].

As more people, devices, and personal data go online, and become interconnected, there is an increasing focus on one essential element of this new digital environment - our identities.

1. The ability to prove that we are who we say we are is more and more critical for us to establish trust in each other and to make significant interactions in the digital economy. If done correctly, an identity framework could surface transformative opportunities, such as citizen's access to basic services and more customized digital experiences. It could also improve health and well-being through access to services, better traceability in supply chains, and security for citizens.
2. However, we are still learning what "identity in a digital world" means.
3. Governments and industry have also been developing policies and best practices regarding the collection, processing, and use of data related to identity, with the aim of increasing opportunities for individuals without encroaching on their freedom or causing harm.
4. Nonetheless there is significant space for improving the way data related to identities is handled online, and how much control the individual has in the process.
5. Here, it is worth highlighting the fact that, when thinking about digital identity, we

need not see it as a unique thing. Digital identity is the total sum of all the attributes that exist upon us in the digital world, an ever-growing and evolving collection of data points.

6. There are increasingly serious and persistent issues in the way these digital identity systems work today.

Overview of the Current Identity System in Brazil

Nowadays, the identity system in Brazil is still predominantly analogical and quite fragmented. This is because biometrical civil identification data is not unified in the country; for example, Brazil does not have an integrated registry of fingerprints.

This creates a system in which citizens can use different (physical) identity cards in any place across Brazil.

Such a system could enable a malicious person to make multiple (physical) identity cards and use them across each state. This is problematic because all of them could have the same fingerprint, but with different names and data associated with it. This problem is due to the lack of biometrical integration among the states.

For instance, a "Potiguar" - a person who was born in the state of Rio Grande do Norte, in the North of Brazil - may use data of a "Paulista" - a person who was born in the state of São Paulo - to make his or her identity registration in Rio de Janeiro. That occurs because the biometrical civil registry is a statewide attribution (not federal), which is also the reason why each state has its own regulation and

levels of maturity. In addition, such a process of integration would be an expensive and troublesome process.

Members of the military forces are in a separate identification data bank, which the other state agencies can't access. If the police arrest someone without an identification card, that arrest will be attributed to the data that the person registered at the time of the arrest.

In spite of where the system might be lagging behind, digital identification has advanced in some ways in Brazil.

For example, Brazil is one of the few countries where the state has created an infrastructure for public keys - Infraestrutura Brasileira de Chaves Públicas - ICP-Brasil (the official PKI in Brazil.) - legally established by the provisional measure 2,200, emitted for the last time on August 24, 2001.

Another positive point is that the Brazilian method of identity management allows for checking the expiration date of the signature and the integrity of identity documents.

Furthermore, since 1997 [2], Brazil has been preparing to launch its national service of digital identity and has advanced a schedule of data interoperability.

In 2008, the Superior Electoral Court (Tribunal Superior Eleitoral - TSE, in Portuguese) started registering the voting of citizens, now with their biometrical information.

Later, in 2017, the DNI project was approved by federal law - Lei Federal No 13.444/2017

[3] - which created a National Civil Identification - Identificação Civil Nacional (ICN). The tests were performed in 2018 with the TSE team, by testing digital identification with members of the parliament, and federal civil servants who registered in May of 2018.

Using the biometric databank of the Electoral Justice as a base, around 100 million Brazilian citizens - from a total population of over 210 million people - had their biometric data captured by TSE and it's been maintained ever since. Aside from the information regarding voting cards, the Brazilian repository of digital IDs is being launched with social security data.

As stated by TSE, the data of the ICN program could be used by the National Institute of Social Security - Instituto Nacional de Seguridade Social (INSS) - to reduce social benefits fraud.

According to the agency responsible for the program of National Civil Identification (ICN) [4], the Superior Electoral Court (TSE) Brazilian states are currently being evaluated and prepared for the implementation of a national digital identification system.

The project foresees the inclusion of documents, such as driver's license, birth and marriage certificates, as well as data from public health registries and, eventually, identification cards - which every Brazilian citizen already owns.

It is expected that the implementation of the digital identification system in Brazil will be completed this year, 2020.

The International Landscape

The United States of America

According to the report [5] published by The Better Identity Coalition (an organization focused on the development of the best solutions for the verification and authentication of identity) US\$ 16.8 billion were lost in the United States due to identity fraud in 2017 and in the same year there was an increase of 44.7% in the number of data violations.

Almost 179 million registries containing personally identifiable information (PII) have been exposed, which illustrates the inadequacy of the current identity systems.

The report presents a set of recommendations for consensual policies, intersectoral, and agnostic of technology ("Policy Plan") for approaching current inadequacies and improving the digital identity infrastructure in the United States.

Estonia

Estonia has one of the most advanced systems of digital identification in the world. Beyond an identity document with a legal picture, the mandatory national card also offers digital access to all the electronically secure services of Estonia. 98% of the Estonian population has a "cumulative" digital identity, 67% regularly use ID cards, and 88% frequently use the Internet [6].

The card chip carries embedded files and, using 2048 bit public-key cryptography, it can be used as definite proof of identification in the electronic environment

Here are some examples of how it is regularly used in Estonia [7].

- legal travel identification for Estonian citizens who travel inside the EU
- national health security card
- proof of identification when logging into bank accounts
- digital signatures
- i-vote
- checking medical registries
- presenting tax declaration
- and more

Estonia sees the next natural step in the evolution of the electronic state as a total transfer of essential services to the digital world.

World Economic Forum

The World Economic Forum has an initiative called Shaping the Future of Digital Economy and Society [8] consisting of a global platform of cooperation to establish a sustainable, inclusive, and reliable digital economy.

This global platform of cooperation has the aim of reaching six results on a worldwide level. They are:

1. Access and adoption - everybody - with no geographical differences of gender or income - may access and use the Internet.
2. Responsible digital transformation (businesses, governments, and leaders of the civil society must act with responsibility and competence to promote a sustainable digital transformation.)

Fit for purpose, informed governance (worldwide, regional, and national policies are informed by pieces of evidence and well equipped to deal with the transnational nature of the digital connectivity.

3. Safe and resilient people, processes, and practices (all individuals, institutions, and infrastructure are resilient to vulnerabilities created by the increase of digital connectivity.)
4. Digital identities focused on the user and interoperable (people can access and use included systems of digital identity that enhance their social and economic well-being.)
5. Reliable data innovation (institutions may share data to create social and economic value, respecting the privacy of digital citizens.)

Taking these six guidelines as a base for an inclusive and reliable sustainable digital world, a digital economy, at the Annual Meeting of the World Economic Forum of 2018 in Davos, a diversified group of interested parts, public and private, made the commitment of collaborating to promote sound digital identities centered on the user.

Through this, the Platform for a Good Digital Identity has emerged, aiming to advance the global progress toward digital identities that satisfy at least five criteria.

Criteria for the Platforms for a Good Digital Identity

According to the World Economic Forum, a good digital identity must be fit for the purpose, inclusive, useful, safe, and offer options to the individuals.

Such will be done through the advance of collaborative initiatives in six significant areas [9]:

1. Moving the emphasis to providing value to

- the user, instead of just capturing identity.
2. Creating metrics and responsibility for a sound identity.
3. Creating new models of governance for ecosystems of digital identity.
4. Promoting the stewardship of sound identity.
5. Encouraging partnerships around the best practices and interoperability of identity, when appropriate.
6. Innovating with technologies and models and constructing a library of successful pilot instances.

Indicating paths

1. Build up new structures of identification based on the concept of decentralized identities. Due to a combination of technological advances, including an increasing sophistication of smartphones, advances in cryptography, and the advent of blockchain, now, an interesting subset of decentralized identities is feasible.
2. Developing a self-sovereign decentralized digital identity system where the user controls not only the identity but also the data associated with it, what is known as Self Sovereign Identity (SSI).

On an SSI approach, the user has a way of generating and controlling exclusive identification, as well as some facilities to store identity data. The users become free to use the identity data as they like. These may be verifiable credentials, but these may also be data from a social media account, historical transactions in an electronic trade website, or mechanisms of verification from friends or colleagues. It has no limits.

3. Awareness that digital identity is the total sum of all the attributes that exist about us in the digital world, a collection of data in constant increase, and points in evolution.
4. Establishing international coordination and the harmonization of patterns of identity.
5. Instructing consumers and companies regarding better digital identity solutions.
6. Governments should seek partnerships with the industry to educate consumers and companies regarding modern approaches and better practices in identity protection and validation.

An example of a potential partner that we have to consider is the National Cyber Security Alliance (NCSA), which already has

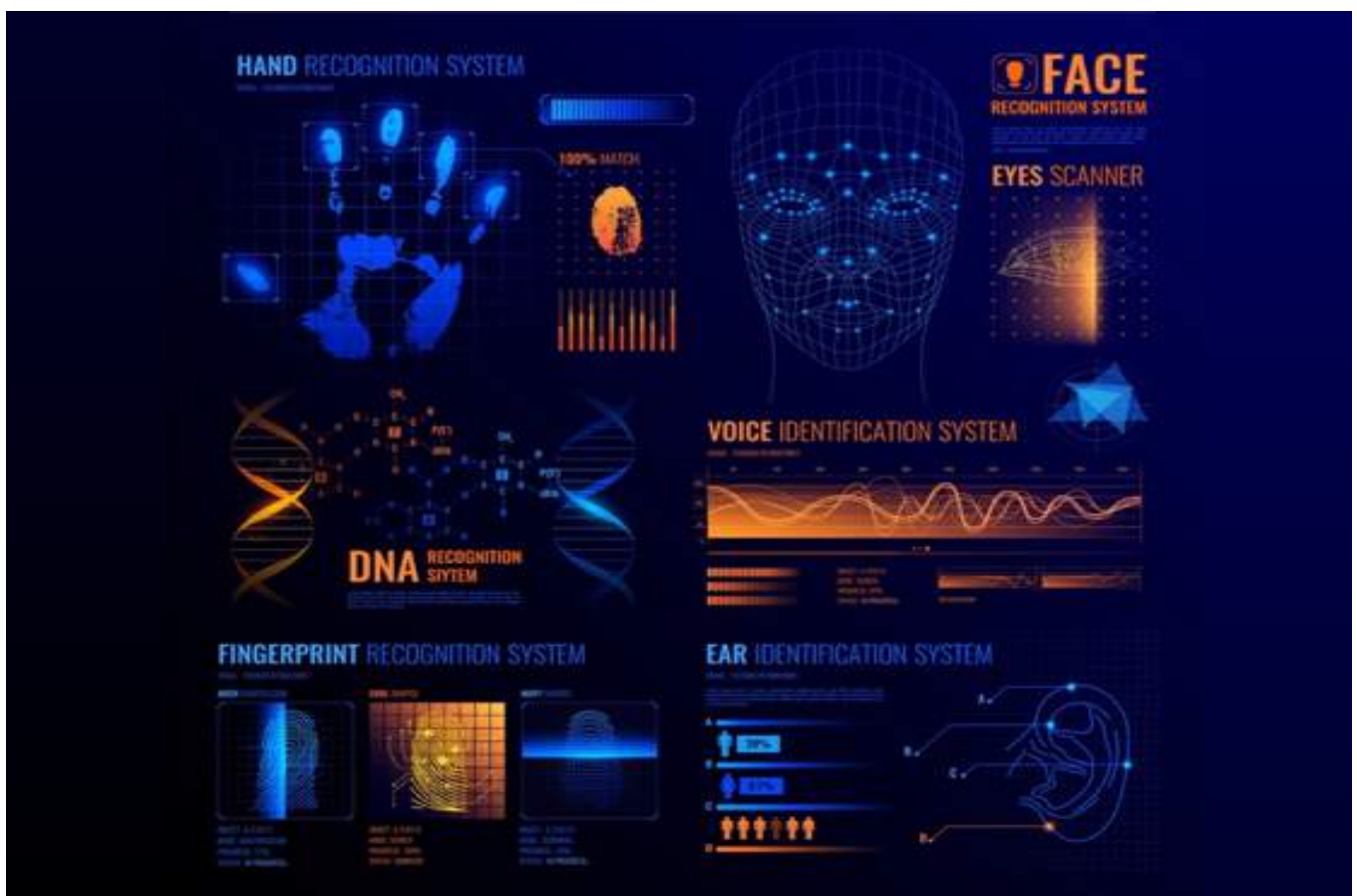
a strong portfolio in the handling of public-private partnerships to make the public aware of cybernetic security.

Blockchain - a powerful solution for different aspects of the decentralized identification structure

Regarding perspectives and insights about digital identity, there are unrelenting - and more and more serious - issues in the way digital identity works today.

Most of the problems related to digital identity are not associated with technology, though, but to the processes.

The shift from a centralized Internet (Web 1.0 and 2.0) to a decentralized Internet (Web 3.0) has already begun. It is not by accident that many countries have adopted a paradigm of



decentralized identity, especially Europe - with the goal of putting the user at the core, thus removing the need of third parties issuing and managing identity.

In the world of decentralized identities, the users create their own digital identities. That usually starts with a user creating his or her own exclusive identifier or identifiers, and then attaching information to that identifier in order to validate its authenticity. In this process, the user can collect credentials from trusted authorities, and produce them when necessary.

While Blockchain is not necessary for decentralized identity, it may be a powerful solution for different aspects of the decentralized identity structure. It could work as support for the creation and registration of digital identities (DIDs), notoriety accreditation, a source for a decentralized infrastructure for identity access, control and consent for the use of the data, and potential propagation of credentials to smart contracts, for instance, to make automated payments. decentralized identity, it may be a powerful solution for different aspects of the decentralized identity structure. It could work as support for the creation and registration of digital identities (DIDs), notoriety accreditation, a source for a decentralized infrastructure for identity access, control and consent for the use of the data, and potential propagation of credentials to smart contracts, for instance, to make automated payments.

Although technical and pattern developments are, with no doubt, significant for the implementation of a new digital identity structure, the legal and regulatory issues are fundamen-

tal. This importance of this becomes especially imminent when we consider that our identity touches so many critical elements of our personal and economic lives.

Conclusion

In conclusion, for the promotion of an ideal digital identity system, public law and policy-makers could:

1. Clarify the "gray area" of regulatory issues, especially around the position of signatures based on new technologies like blockchain and timestamps under eIDAS.
2. Create a framework for decentralized digital identities while instructing government agencies and encouraging them to get involved in these developments, for example, as issuers of verified credentials.
3. The government can and must play an essential role as an issuer of verified credentials.
4. Legislators must modernize the legislative framework reference to the platforms of digital authentication and reduce the barriers to the adoption of innovative security systems.
5. Elucidate open issues around decentralized identity.
6. The new legislation regarding privacy, data protection, and security should not be written in such a broad way that could prevent the use of promising technologies for validation based on risks.
7. Governments need to give special attention

to cybersecurity and the migration of cybernetic risk, creating detection systems and protection against invaders, practicing cooperation with public and private institutions, thus significantly contributing to the awareness of the users, and taking part in the immense international collaboration.

I wrote this text for my participation in the panel "Digital Identity" at the World Legal Summit (WLS2019), which took place in Belo Horizonte, Brazil, on the 1st of August, 2019. I thank so much the Law Commission for the Startups of the OAB-MG for the invitation.

#digitalidentity #DID #self-sovereignid #digitalid #blockchaintechnology #blockchain #government

Suggestions and comments are always welcome.

References

- [1] Blockchain and Digital Identity - European Observatory
- [2] when it was determined to merge registration systems at the state level into a future unified ID registration.

[3] <https://www2.camara.leg.br/legin/fed/lei/2017/lei-13444-11-maio-2017-784695-publicacaooriginal-152527-pl.html>

[4] <https://www.zdnet.com/article/brazil-attempts-to-advance-unified-id-project/>

[5] Better Identity in America: A Blueprint for Policymakers (the "Report"):

<https://static1.squarespace.com/static/5a7b7a8490bade8a77c07789/t/5b4fe83b1ae6cfa99e58a05d/1531963453495/Better+Identity+Coalition+Blueprint+-+July+2018.pdf>

[6] <https://e-estonia.com/solutions/e-identity/id-card/>

[7] <https://e-estonia.com/solutions/e-identity/id-card/>

[8] <https://www.weforum.org/system-initiatives/shaping-the-future-of-digital-economy-and-society>

[9] <https://www.weforum.org/projects/digital-identity>

About the Author

Tatiana Revoredo is Founding Member at Oxford Blockchain Foundation. Liaison at European Law Observatory on New Technologies. CSO at the Global Strategy.






WLS Brazil



WLS Minsk

Suggested legislative measures to overcome the contract tracing “trust gap”

By Mark Potkewitz, Lawyer and Director of the Legal Innovation Centre at Ulster University
and Ryan Carrier, Executive Director of ForHumanity



As nations struggle to roll out contact tracing solutions that rely on common consumer electronics, many lack important legal safeguards to prevent contact tracing data from being used for other purposes like criminal investigation, mapping networks of protest or dissent, and other purposes that could compromise special relationships, such as between lawyers and their clients.

Contact Tracing refers to a strategy often taken by healthcare professionals to identify individuals who have risked exposure to infectious diseases. In the past, persons acting as contact tracers would rely on a patient's memory of where they had been or with whom they had come into contact. The tracers would then contact those individuals and/or places to try to map out an ever-widening net of individuals who could be at a higher risk for contracting the disease.

Researchers have already identified a number of "wish list" use cases for the data collected by contact tracing programs. While the temptation exists to use data collected through contact tracing programs for a wealth of beneficial research, governments have a long track record of mission creep, overreach and broken promises. Contact tracing is too important; it is too valuable to the toolkit for pandemic response to allow these missteps regardless of good intentions such as "valuable data for research" or "we could learn so much". Researchers have at their disposal a range of means to acquire data for other purposes and social or clinical investigation. Once a useful contact tracing solution has been developed, government authorities can "clone" the solution, repurpose it, and relabel it for collection of research data wholly independent from pandemic contact tracing. Rumblings of using contact tracing data for *other* purposes serve only to feed public speculation and erode public confidence and trust.

Researchers have already identified a number of “wish list” use cases for the data collected by contact tracing programs. While the temptation exists to use data collected through contact tracing programs for a wealth of beneficial research, governments have a long track record of mission creep, overreach and broken promises. Contact tracing is too important; it is too valuable to the toolkit for pandemic response to allow these missteps regardless of good intentions such as “valuable data for research” or “we could learn so much”. Researchers have at their disposal a range of means to acquire data for other purposes and social or clinical investigation. Once a useful contact tracing solution has been developed, government authorities can “clone” the solution, repurpose it, and relabel it for collection of research data wholly independent from pandemic contact tracing. Rumblings of using contact tracing data for *other* purposes serve only to feed public speculation and erode public confidence and trust.

Trust has remained an issue through the historical, analog process of contact tracing. Vulnerable patients could be told they must reveal the names of the people with whom they had been in contact, where they had been, and when they had been there. Intimate personal relationships, membership in certain communities or organizations, and clandestine gathering places could become exposed through contact tracing. Were I to reveal the names of people with whom I had recently come into contact, their names could forever be emblazoned in the rolls of some contract tracing authority without their having ever given consent.

As we consider the merits of technology in contact tracing, we must recognize that additional trust issues emerge when we confront technology and data placed in the hands of the government or our employers. While we see efforts to “track and map social networks”, and promises from governments to “ring-fence datasets” while ensuring “future data deletion”, we lack an appropriate means of ensuring these promises are kept. In short, right now, we cannot see the watchmen across the widening “trust gap”.

According to experts, the adoption efficacy threshold for contact tracing to become effective must run above 60% of a given population. [1] However, current adoption in island nations like Australia and Singapore appears to have peaked at 25%. [2] In the United States, only 20% of total participants in a Brookings Institute survey said they would “strongly support” a contact tracing app compared to 36% who “strongly opposed”. [3] Only 19% of respondents were “extremely likely” to download a hypothetical contact tracing app while 42% said they were “extremely unlikely”. [4]

Why such a negative response? Researchers found that “The technology [...] elicits visceral reactions about whether it can adequately preserve privacy.” [5] A “trust gap” clearly presents a significant barrier to widespread adoption of contract tracing.

Public authorities can work to overcome the “trust gap” by taking 3 simple steps:

- Independent audit and oversight;
- Statutory and judicial remedies addressing

- misuse of contact tracing apps or their related data; and,
- Legal commitments to data deletion

Since [independent audit](#) and deletion have been covered elsewhere, this paper will focus on the types of statutory protections that can help minimize the risk that contact tracing data be used for purposes beyond public health applications.

The contact tracing process can function in a similar fashion to the extensive link analysis undertaken by the US National Security Agency using telephony metadata from large carriers like Verizon. The NSA would use “three hops” to map out networks of people centered around a targeted individual. For instance, I call my brother (first hop), my brother calls for a pizza delivery (second hop), and now anybody who contacts the pizza place is collected through the third hop.

The parallels between contract tracing and link analysis undertaken in the signals intelligence community have alarmed many civil liberties and privacy advocates. Because of the dangers presented by COVID-19, many jurisdictions have favored rapid development and deployment of solutions rather than a more considered, contemplative approach backed by legislative protections for the public who may share with governments an unprecedented amount of information about their private lives.

In order to bridge the “trust gap”, nations should consider elevating contact tracing as a tool of public health to a special, privileged status beyond the reach of a general warrant

or subpoena. Lingering, mission creep, and authoritarian overreach will be devastating to this tool. “Ring-fencing” is an insufficient term. These should be “Castle Wall-fencing and let’s put the moat in to be sure”. Nations that treat contact tracing in this manner will come to realize tremendous value as the “trust gap” is bridged and adoption and compliance are swift for the next pandemic/epidemic.

In response to the chorus of voices calling for greater oversight and security for contact tracing, some jurisdictions have begun to pass legislation to protect the people’s information. In other jurisdictions, steps have been taken to prevent movement or entry restrictions based on app usage. Unfortunately, much of this legislation falls short of substantial protection. However a few jurisdictions have taken a more comprehensive approach. These efforts enshrine via statute important privacy protections for contact tracing subjects and their data while putting forward positive steps to punish misuse and improper sharing of data. Australia’s *Privacy Amendment (Public Health Contact Information) Act 2020* is one of the best we have seen thus far. [6] In order to foster greater public trust and proceed in a spirit of transparency, jurisdictions should consider inclusion of provisions via statute or regulatory measure that address the following concerns:

- *Explicit restrictions on how government may use contact tracing data:*

While this element appears rather straightforward, some jurisdictions have relied on vague and broad language to describe how they may use data collected via contact tracing programs. Absent explicit and specific language delimiting the manner in which the

collected data may and shall be used, people lack appropriate protections to ensure that their data does not later become used to discriminate against them, for instance, stricter quarantining in some future epidemic or some form of healthcare discrimination with regards to future treatment if COVID-19 proves to have long-term health ramifications for those exposed. [7] Despite the temptation to use the data for other research purposes, this should be prohibited.

- *A suppression remedy for data improperly shared with law enforcement:*

In the United States, for instance, Courts will often exclude or suppress evidence obtained in an illegal or unlawful manner. A jurisdiction that has passed social distancing rules may want to impose a fine on those who do not strictly adhere to those rules. If contract tracing app data already sits within a government agency or instrumentality, it can quickly become the basis for investigation, fining, or prosecution of protestors who break isolation rules. A suppression remedy can prevent the use of contact tracing data for law enforcement purposes.

- *A private cause of action against contact tracing entities and service providers with a negligence standard and statutory damages:*

While this may be the least likely measure to gain adoption, it would give individuals the ability to sue a contract tracing entity and/or its service providers for improper data sharing, leaks, or breaches. Since the collection and sharing of contact tracing data presents several opportunities for improper safeguarding, storage, and sharing

of data, several providers involved in the process can become the source of data improperly shared with government agencies or the public. Legislation that allows individuals to sue a contract tracing authority and its service providers for *negligently* sharing the data can cause contact tracing authorities and their service providers to take more care in how they handle people's data.

- *A statutory right to a Data Subject Access Request:*

Under the GDPR and other similar pieces of legislation, people have a right to request certain information from entities holding their data such as a copy of all the data held, and other information about how it was collected and used. People sharing their data for the purposes of contract tracing should have the ability to get a clearer understanding of what the data collected from them and held about them.

- *Clear and controlling legislation or regulation which states how contact tracing data will be used in any aggregate or anonymized form with associated consents:*

Large-scale contact tracing solutions can provide researchers with an incredible wealth of information that can become a tempting area for study and analysis to explore large groups of people and how they move through settled space. What makes app-based contact tracing different from simple geolocation data is the actual proximal links between specific individuals and social/kinetic/geographical relationships between individuals. One could see the

value to a public transit system for instance, of post-lockdown contact tracing data to get a better understanding of things like bus routes or subway station activity. This same type of information could arguably be useful to law enforcement to evaluate how people move through high-crime areas in space and time, to identify high-traffic areas for enforcement of current and future lockdowns, and locate strategic points for surveillance measures. Without clear and simple explanations of how this data will be used, people cannot grant meaningful consent to collection of their data. Authorities must demonstrate that they protect the value of contact tracing as a tool of public health by avoiding the temptation to use good and interesting data for additional purposes like research. We advise they seek it from other sources with explicit consent from users. *Save contact tracing for public health.*

- *Criminal or civil punishments or sanctions for misuse or improper sharing of contact tracing data with an appropriate mens rea standard:*
Jurisdictions should consider how appropriately to deal with the improper use or improper sharing of contact tracing data. A range of sanctions should exist to punish a range of contact tracing data offenses. The punishments available should scale in a fashion concomitant to the offense. Negligence should not be an excuse for improper data sharing or data usage.
- *Criminal or civil punishments or sanctions for knowing misuse of a contract tracing solution or knowingly reporting false information:*
People should not be permitted to knowingly

report false information to a contact tracing application (such as reporting themselves as COVID-19 positive if they know or have reason to know that they are not COVID-19 positive). [8] While people may not want to divulge certain information to manual contact tracers, they should certainly not knowingly report *false* information.

- *Legislation which directly suspends any data retention rules and guarantees deletion of data to the highest extent of the definition of deletion:*
Some jurisdictions have rules that require the maintenance of certain types of records for statutory periods of time, like the Sarbanes Oxley Act with certain business records and tangible objects, or tolling records maintained by telecommunications carriers required by the Federal Communications Commission. Some jurisdictions have separate rules for data collected by government agencies or separate rules based on the nature of the data, such as health or business records. Statutory exclusions for contact tracing data from existing record-keeping laws would go a long way to increase public trust.
- *Non-discrimination clauses:*
Admittedly, this does not relate to barriers to adoption based on the trust gap, but it does speak to the general public attitude toward the effort. Jurisdictions will need to consider where enrolment in a contact tracing program will serve as a requirement for the enjoyment of public services, such as libraries, public transit, or public schools, or public accommodations, such as hotels, movie theatres, and sporting arenas. What if private

enterprises generally available to the public, such as bars, restaurants, and stores try to require proof of contact tracing enrollment as a means of demonstrating lack of exposure before admittance?

The foregoing, non-exhaustive list of suggested reforms neither addresses nor solves every issue presented by contact tracing. However, together they can help bring greater protections for the public, transparency around the collection, storage and use of contact tracing data, and accountability for those involved in the execution or delivery of contact tracing solutions.

With a handful of simple steps, governments can lower barriers to adoption by reassuring the public that data will be used for a limited range of public health purposes, and that any current or future/intended use of the data be made clear and explicit to those affected by contact tracing programs.

Notes

[1] Sarah Kreps, Baobao Zhant, Nina Murray, [Contact-tracing apps face serious adoption obstacles](#), TECH STREAM, Brookings Institute, May 20, 2020.

[2] Stephanie Findlay, Stefania Palmra, and Richard Milne, [Coronavirus contact-tracing apps struggle to make an impact](#), FINANCIAL TIMES, May 18, 2020.

[3] *Id.*

[4] *Id.*

[5] *Id.* Pew Center researchers found similar results: Just over half of adults surveyed felt it acceptable to use cellphones to track those who tested positive for COVID-19, while 48%

believed it was not acceptable. Brooke Auxier, [How Americans see digital privacy issues amid the COVID-19 outbreak](#), FACT TANK, Pew Research Center, May 4, 2020. Within those numbers, only 24% felt it was *very* acceptable as compared to 33% who felt it *very unacceptable*. *Id.* The numbers of those who find cell phone tracking somewhat or very unacceptable grows when asked about tracking those “who may have had contact with somebody who has tested positive for the coronavirus” and increases further when asked whether the technology should be used for enforcement of expert advice regarding physical distancing and isolation. *Id.*

[6] [Privacy Amendment \(Public Health Contact Information\) Act 2020](#).

[7] However, certain circumstances may exist where government may need to investigate improper or malicious use of a contact tracing application by those seeking to weaponize contact tracing to harm rival businesses, strike back at personal or romantic competitors, or falsely identify certain geographic areas as *high risk*. In addition, a circumstance may arise in which a criminal defendant using a contact tracing application may want to use geolocation and/or exchanged token information to supply an alibi to prove their location or identify witnesses if accused of a crime. Use of the data in these instances should be permitted.

[8] This does not speak to whether people should be compelled to report that they are COVID-19 positive if they know or have reason to know that they are. So far, it appears that most apps rely on users to report only when they have tested positive or are experiencing symptoms of COVID-19 rather than needing to affirm non-exposure or lack of symptoms.

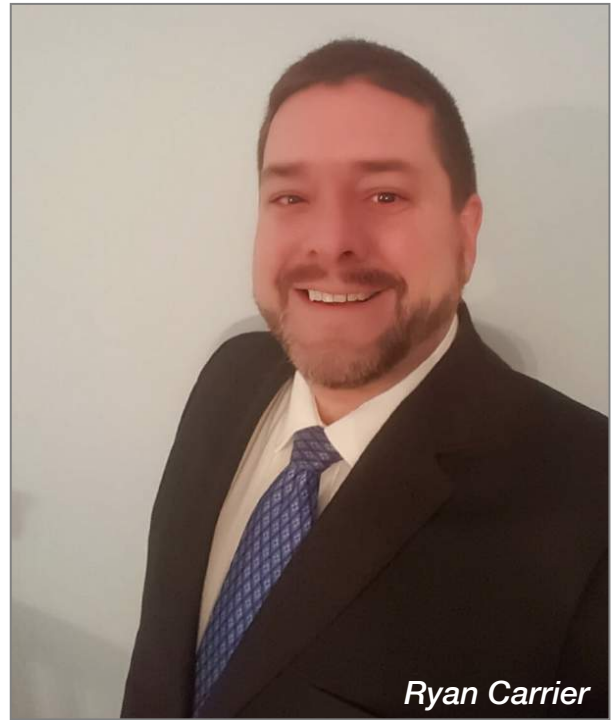
About the Authors

Mark Potkewitz is an attorney with a background in federal legislative policy and Director of the Legal Innovation Centre at Ulster University, as well as a Fellow with ForHumanity.



Ryan Carrier is the Executive Director of ForHumanity, After a 20+ year finance career in-

cluding time with the International Finance Corp, Standard & Poor's and Macquarie Bank, he founded ForHumanity to examine and analyze the downside risks associated with the ubiquitous advance of AI & Automation. Further, to engage in risk mitigation, where possi-



ble, to ensure the optimal outcome...ForHumanity.



**MORE MAGAZINES ON THE
BUSINESS OF LAW
GO TO OUR LIBRARY AND READ
OR DOWNLOAD YOUR COPY(S)**

A Proposed Framework for the Auditing of AI Systems

“To examine and analyze the downside risks associated with the ubiquitous advance of AI & Automation. Further, to engage in risk mitigation, where possible, to ensure the optimal outcome... ForHumanity”

ProtoType First Use Case: Contact Tracing Technologies

In response to the COVID-19 pandemic, there is a growing body of contact tracing technologies and no real way of ensuring their governance. We are aiming to fix that, and invite you to take part in this prototype *Independent Audit of Contact Tracing*.

We’re proposing a framework that audits for:

- **Privacy**,
 - **Ethics** (Contact Tracing Authority, Launch, Population Covered),
 - **Trust** (Disclosure, Transparency, Control, Safety),
 - **Bias** (Age, Ability, Guardian),
- and much more.



ForHumanity Fellow

Adam Leon



ForHumanity Fellow

Ryan Eagan

1	Independent Audit of Contact Tracing v1.6
2	This document is the property of ForHumanity Inc. (c)2020, ForHumanity Inc. a 501 (c) 3 tax-exempt Public Charity
3	All rights reserved
4	Bold, Black and Capitalized = Defined Word, found on tab "Definitions"
5	Privacy
6	Is Personal Data being collected?
7	Is Sensitive Personal Data being collected?
8	Is the data collected being aggregated by the CTE?
9	Is the data collected being aggregated by the Contact Tracing technology itself?
10	Is the CTE examining or analyzing individual data?
11	Is the CTE examining or analyzing the aggregated data?
12	Ethics - Contact Tracing Authority/Launch/Population Covered
13	Is a Pandemic necessary for your entity to initiate a Contact Tracing program?
14	Has a Global Health Authority or National Health Authority declared a Pandemic ?
15	Is an Epidemic necessary for your entity to initiate a Contact Tracing program?
16	Has a Global Health Authority or National Health Authority declared an Epidemic ?
17	What are the requirements for a Contact Tracing program to be initiated?
18	Does the Contact Tracing Entity (CTE) have the authority to call a Pandemic or Epidemic ?
19	Does the CTE have the authority to contact trace ?
20	Trust - Disclosure/Transparency/Control/Safety
21	For all service providers to the CTE is their contract publicly available?
22	Are there multiple layers of consent in the Contact Tracing technology?
23	Is there consent on download of the app?
24	Bias - Age/Ability/Guardian
25	Is Age collected by the Contact Tracing system?
26	Is an Age range collected by the Contact Tracing system?
27	Is Age used by the the Contact Tracing technology to differentiate the response or reaction of the system?
28	Is Age used by Contact Tracers to differentiate the response of a Contact Tracer ?
29	Is sexual orientation a variable collected by the Contact Tracing system?
30	Is gender a variable collected by the Contact Tracing system?
31	Is religious belief a variable collected by the Contact Tracing systems?
32	Is income level a variable collected by the Contact Tracing systems?
33	Cybersecurity (based and adapted from NIST Guidelines)
34	Does the CTE have a monitoring program for look-a-like app attacks?
35	Does the Service Provider conduct vulnerability tests?
36	Does the CTE conduct vulnerability tests?
37	Does the CTE review latest threat intelligence?
38	Does the Service Provider review latest threat intelligence?
39	Is there a risk assesment on new threats tested against the system?



ForHumanity Fellow

Alexa Anastasia



ForHumanity Fellow

Mark Potkewitz



ForHumanity Fellow

Dr. Aaron Maxwell



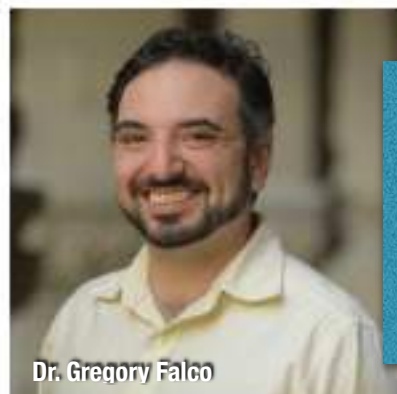
ForHumanity Fellow

Dr. Shea Brown



ForHumanity Fellow

Dr. Dorothea Baur



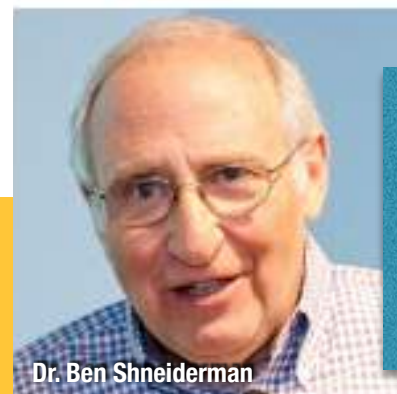
ForHumanity Fellow

Dr. Gregory Falco



ForHumanity Fellow

Paolo Cecchi



ForHumanity Fellow

Dr. Ben Shneiderman



ForHumanity Fellow

Dr. Gisele Waters

Audit Backup	IAAIS Classification	Best Practice
Document/Test	Privacy	
Document/Test	Privacy	
Document/legislation	Privacy	
Document/Test	Privacy	
Document/legislation	Privacy	
Document/legislation	Privacy	
Provide legal authority	Ethics	Yes
Provide official evidence	Ethics	
Provide legal authority		
Provide official evidence		
Provide legal explanation	Ethics	
Provide legal explanation	Ethics	No
Provide legal explanation/Budget	Ethics	Yes
Document	Trust	
Document/Test	Trust	Yes
Document/Test	Trust	Yes
Document/Test	Bias	
Document/Test	Bias	Yes
Document	Bias	
Document	Bias	
Document/Test	Bias	No
Document/Test	Bias	No
Document/Test	Bias	No
Document/Test	Bias	No
Sample Output	Cybersecurity	Yes
Test	Cybersecurity	Yes
Test	Cybersecurity	Yes
Document	Cybersecurity	Yes
Document	Cybersecurity	Yes
Test	Cybersecurity	Yes



WLS Singapore



WLS Cape Town



WLS

WORLD LEGAL SUMMIT

GET INVOLVED

info@worldlegalsummit.org