WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Industry Agenda

Information Technology and Telecommunications Industries

Annual Meeting of the New Champions Summary Report

On 11-13 September, the Information Technology and Telecommunications Industries Partners convened for a series of private sessions to discuss the future of the industry and explore the implications of the large-scale changes that the industry is facing today.

The ICT Strategy Meeting focused on how stakeholders are shaping the future of the industry and on the most pressing issues for the Industry Partners. The Partnership for Cyber Resilience session examined the implications of cyber-threats in potential scenarios. The New Data Commons session discussed evolving data governance models. The Delivering on Digital Infrastructure session identified traditional and non-traditional infrastructure providers and considered the scenarios of digital infrastructure development.

REF 281013

ICT Strategy Meeting

Key Issues

- Which stakeholders are missing from the global industry dialogue?
- How should businesses operate in emerging markets?
- What is the role of IT industry regulation?
- How are the value and governance of personal data changing?
- How can better cooperation between governments and the industry be ensured?

Synopsis

As technology increasingly becomes an enabler, the leaders of the industry must focus on the areas that are both greatly uncertain and highly impactful. The meeting began with a discussion on the need to work more effectively in emerging markets and to better understand the ongoing evolution of digital infrastructure.

The key area of uncertainty and concern for businesses operating in emerging markets is regulation. Many companies are faced with contradicting regulations around the world. In some countries, regulation is a means to keep industry players out of the market, to protect the market or to "enforce a certain way of thinking". Finding the right business models in emerging markets and how to replicate them elsewhere are key factors to scaling businesses. The industry leaders underlined their interest in doing business better in these markets and in keeping up with customers' expectations of high-quality services.

Privacy and security remain other areas of uncertainty for most companies. As user and government awareness of these issues grows, the heads of industry are keen to help shape emerging privacy norms. New norms regarding privacy are likely to significantly impact most ICT companies' business. The companies, on the other hand, have to be more flexible and agile in managing risks. It was noted that privacy is a "personal" and an "organizational" matter, whereas data sovereignty is an issue at the national level. As one norm is drafted on top of another, a layering of privacy norms is occurring.

01: Participants of the ICT Strategy Meeting
02: Orlando Ayala, Chairman, Emerging Markets, Microsoft

Consumers are often unrepresented in the emerging dialogues on privacy. Face and voice recognition technologies are reaching the point where “they actually work”. There is also a growing understanding that individuals should have the right to remain anonymous on the Internet. Companies are beginning to think differently about what data can be protected and what assets are at stake.

It is also noteworthy that technological literacy and an understanding of technology’s implications are growing fast among users. At the same, the view of intellectual property in emerging markets is not the same as in more established markets.

Spectrum management, the process of regulating the use of radio frequencies, and the use of licensed versus unlicensed spectrum is another important issue. Mobile platforms are a growing means of doing business and delivering services. Tablets and mobile phones have become more than just “cool things to have”.

Companies operating in the digital era are working in multiple spaces. Technology is spreading fast and industry “will not wait” to leverage these opportunities. The industry should also think about what bits of technology are unable to be regulated.

Missing from the current dialogue is better cooperation between businesses and governments. No one stakeholder in the dialogue should carry all the weight.

The social media platform is a new and powerful tool that companies can leverage. In the social media space, “clicktivism”, which shows how many clicks, “likes” and shares a post receives, must be distinguished from civil society opinion, as this activity does not necessarily reflect public opinion.

Internet governance belongs in companies’ most important domains. Labour markets, the availability of jobs and the world of work will also change as a result of evolving technologies; robots will soon be capable of replacing much of the work performed by humans. Also, a divide between the countries that consume and those that produce the technology can be observed. Patents are among the indicators of this divide. The industry is looking at where the innovation is happening and what the field’s big transformation incentives are.

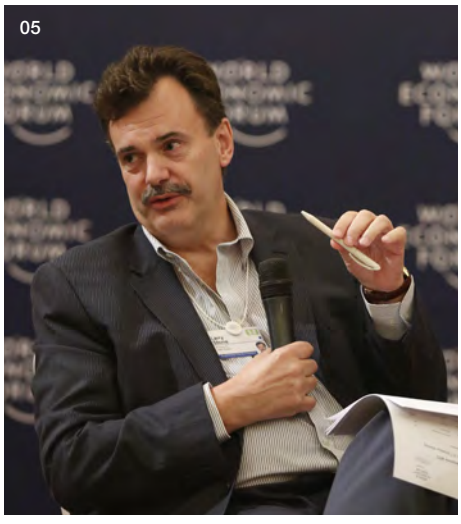

01

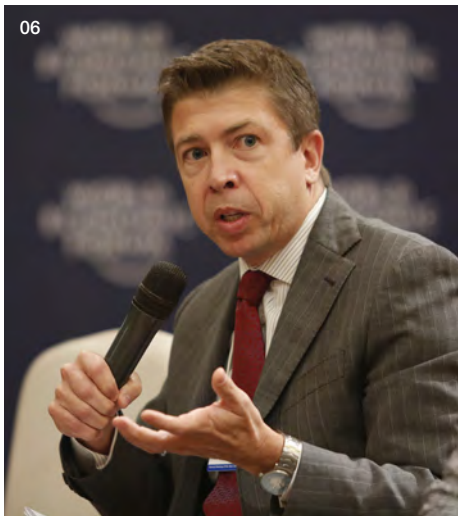

02


03

01: Antonio Viana, Executive Vice-President, Commercial and Global Development, Arm
02: Vic Mankotia, Senior Vice-Pesident, Corporate Strategy and Solution Sales, CA Technologies
03: Anand Chandrasekher, Chief Marketing Officer, Qualcomm
04: Lindsey Held, Vice-President, Global Government Affairs, SAP
05: Larry Stone, President, Group Public and Government Affairs, BT
06: Christopher Mondini, Vice-President, Business Engagement, ICANN


04


05


06

Partnership for Cyber Resilience

Key Issues

- What are the key drivers affecting cyberspace?
- How will cyber-risks unfold in the future?
- What are the potential future scenarios for the world?
- How do businesses and governments operate in these worlds and what are the challenges and opportunities?

Synopsis

The aim of this session was to advance the ongoing efforts of the Partnership for Cyber Resilience, in which over 100 executives have shared their vision of digital risks through executive opinion interviews. Based on feedback from Forum Members and at Partnership for Cyber Resilience meetings throughout the year, the drivers of the cyber-environment and four potential future global scenarios were identified.

Scenario A: Cyber-threats increase but the sophistication of institutions does not.

In this scenario, the number of cyber-threats increases incrementally, affecting every company. Companies devote more resources and implement more stringent controls. Active internal monitoring and testing is in place in some companies. Most companies take a reactive stance and have ad hoc systems for combating severe threats. Innovations (e.g. cloud, enterprise mobility) are adopted more slowly and the exfiltration of intellectual property continues. Public-private and international cooperation is limited.

In this world, security is not built into most products and the sophistication of companies and users is always behind that of the adversaries. Fragmented regulation creates "weak points", and reduced management capabilities drive down the effectiveness of institutions. Users and executives surrender to fatalism, assuming nothing is safe any longer, which decreases innovation and productivity. In this model, it would be necessary to move away from the "fortress" mode to access control models.

Scenario B: Fears about cybersecurity reduce cooperation and trust. Within this world, sophisticated attack vectors are disseminated to a wide range of actors, some with truly destructive rather than parasitic intent.

Governments significantly increase directive or prescriptive regulations with limited coordination internationally, and multinational companies struggle to comply with different regulations across countries. This world may be the world of "unintended consequences". This "worst-case scenario" is very costly. No trust or reliability exists anymore between parties.

Excessive data protection makes running a business and maintaining operations a challenge. Users and companies also start realizing that "governments can't protect everyone", and equivalents of a "neighbourhood watch" mechanism start to emerge. It will mean a "waste of resources" for many institutions and a significant slowdown in global supply chains. From a technical standpoint, many companies might shift back to micro servers. The business of a cloud industry will be significantly disrupted. Massive arbitrage opportunities may emerge in this context. International institutions will play a bigger role, new principles will have to emerge and the world will be in search of new business options to overcome negative effects.


01

01: Participants of the Partnership for Cyber Resilience

Scenario C: Technology and security become enablers of growth but a number of serious abuses take place.

Proactive state action limits the dissemination of sophisticated attacks. There is a dramatic improvement in institutional capabilities (e.g. differentiated protection for most important assets, proactive analytics). Governments facilitate capability uplift (e.g. information sharing). Institutions accelerate the pace of innovation, given the comfort level in cybersecurity. Cooperation on regional and international levels is improved. There is relatively little impact of cyber-risks on innovation, but a number of abuses happen.

Participants agreed that, in reality, "we are already there" and "serious abuses are real". Issues of trust and accessibility are emerging as significant and technology accelerates both "good" and "bad" trends. Government's role would be to provide universal access. Consumers will find it harder to "trust the system", and the ability to conduct commerce and point-to-point communication may be compromised. Permissions to use personal data will be implemented in a much stricter fashion, but a massive disclosure of private data, including biometric data, may happen. Technology can create inefficiencies and a "single point of failure". In this scenario, governments created integrated systems across all agencies and collaborated with industries and citizens.

Public awareness of the risks of technology, expectations from institutions, and pressure on institutions to deliver innovative solutions rise. Multinational companies drive this scenario more than intra-government collaboration, and global institutions develop effective standards. NGOs, the private sector and governments engage in regional and commercial collaboration.

It is not possible to avoid risk 100%, and risk mitigation and analysis will become much more important. Institutions will have to develop plan B instead of "putting all eggs in one basket".

Containment of breaches will be high on the agenda of companies, and institutions will have to become "comfortable with technology". Citizens will expect the "ease of use" of services, and more stakeholders will participate in the global commerce.


01


02


03

01: Omer Laviv, CEO, Athena Security Implementation Christopher Mondini, Vice-President, Business Engagement, ICANN Antonio Viana, Executive Vice-President, Commercial and Global Development, Arm Allen Wu, President, Greater China, Arm Consulting
02: Robert Greenhill, Managing Director, Chief Business Officer, World Economic Forum Christophe Nicolas, Senior Vice-President, Kudelski Group
03: Participants of the Partnership for Cyber Resilience

Scenario D: After destructive attacks, public-private cooperation is improved but consumer trust is eroded.

Several successful attacks on key industry players expose highly personal and sensitive data. Governments work to create effective policy mechanisms of dealing with cyber-threats. Consumer trust is broken. At the same time, several countries ban companies from storing customers' personal data electronically unless there is a clear necessity. Participants discussed whether chief executives would be interested in various insurance options against this scenario. Consumers will be sanguine until the situation is "a lot worse in loss and inconveniences". Participants debated to what extent the broken trust would actually change consumer behaviour. Daily inconveniences would be the biggest problem for consumers. In this scenario, losses can be described either in financial terms or in terms of loss of privacy. For businesses, it will mean pulling back from a number of services, such as cloud services. Opportunities will emerge for new businesses in insurance or mobile security.

For businesses, keeping their customers will become a great challenge. On a macro level, it is recognized that the risks are global, but institutions continue to act locally.

The scenarios exercise showed that institutions are increasingly aware of various types of risks and are in search of sustainable risk mitigation models. Operational improvements, collaborative actions and awareness were identified as some of the main drivers of a secure cyber environment. In the next phase of the project, the Partnership will continue to explore implications and define recommendations.

01: Peter Schwartz, Senior Vice-President, Global Government Relations and Strategic Planning, Salesforce
02: Participants of the Partnership for Cyber Resilience

The New Data Commons

Key Issues

- How can personal data be used to discover new opportunities?
- What are the risks and harms associated with these innovations?
- How can the opportunities available be balanced with the potential risks and harms?

Synopsis

A new approach to managing personal data is needed, one that is centred on the individual and is based on the uses of data rather than the collection of data.

The session opened with a recap of the need for change to achieve a balanced personal data system. Shifting the attention from the collection of personal data to the use of the data would be the appropriate and practical course of action to take in the era of Big Data. The creation of these new systems requires rethinking traditional notions of collection limitations, use specification, and notice and consent – all of which were valid in the past, but are now insufficiently flexible and robust to be effective.

A discussion focusing on the benefits of personal data use, rather than on potential risks, is overdue. Many potential innovations are possible in the personal data space that could bring value to governments, enterprises and society at large.

However, due in part to media coverage, most people are more aware of the risks of personal data use than of the benefits, which impedes progress. Mobile call data records (CDRs) were employed by the United Nations Food Programme's Vulnerability Assessment Mapping to enhance food security risk management and contingency planning. Companies are using CDRs to identify and predict malaria hotspots by linking mobile operator data with disease datasets. This helps to more efficiently plan for and administer vaccinations and other medication. Some companies are using personal data to optimize traffic network and urban planning efforts in emerging markets. Finally, there are examples of mobile operators that have found ways to monetize their signalling traffic in new, innovative business models.

The more data a system has, the greater the potential for innovation. Innovation is driven by need in a given circumstance, which may be different from that in which the data was originally collected. As more data is added to a system and data sets can be flexibly layered, there is greater potential for further innovation.

Risks manifest themselves at different levels. While most businesses have systems in place to identify various classes of risk that impact them directly (financial, operational, etc.), these organizations, in general, are not equally focused on risks to individuals or society.

Regardless of the system or set of controls in place, the potential exists for misuse of data. Whenever a data set is assembled, some degree of misuse is inevitable. Many participants warned of the unintended consequences of legislation that can occur as times and technologies change. Highly effective regulations can have reduced efficacy over time as technologies evolve and circumstances shift. A possible resolution is for all parties to be involved in the design and implementation of policy frameworks.

A common misperception is that the risks of personal data use affect the individual, but the benefits impact society at large. As this misperception is further propagated, it is reasonable to expect that individuals become apprehensive about personal data use and exchange. However, if more is done to communicate the individual and company-specific benefits, public opinion may view personal data use more favourably.

01: Scott David, Executive Director, Law, Technology and Arts Group, University of Washington
Stephen Cross, Executive Vice-President for Research, Georgia Institute of Technology
02: Brett Rierson, Director, China Office, WFP

01

02

Balancing the risks to individuals, businesses and society with the benefits that each of these groups receive was viewed as a key priority. It is necessary to have a robust risk management system that does not stifle innovation in the personal data space.

Encouraging the development of new, exciting data visualization tools was one suggestion to more effectively connect with individuals, which is in keeping with the notion that increased engagement of the individual must be a central priority. If individuals have a way of viewing with whom their data has been shared and for what purpose, they could be more engaged in managing their own risk exposure.

Technological innovations are also at the heart of a robust system. Advances in the way that data are anonymized and aggregated have the potential to enhance individuals' privacy protection while still allowing researchers, government agencies, businesses and other stakeholders the flexibility that they need to innovate. A potential system could feature permissions that are coded into the data and automatically detect the allowability of a forward transfer or use. Finally, legal tools could be updated by borrowing established conventions from other fields to create stronger legal protections that can be practically implemented, developed and enhanced.

To develop a policy framework to underpin these, additional socialization and dialogue is necessary. Legal experts, personal data and privacy experts, and policy-makers from multiple geographies should all be consulted to ensure that any set of solutions is truly global in nature and can be successfully implemented in practice.

Just as important is the participation of the practitioner community. Businesses, governments and social organizations that use personal data to innovate and address key challenges are vital in ensuring that new tools and approaches fit the needs of those who will be employing them.

04

05

01: Participants of the New Data Commons
02: JP Rangaswami, Chief Scientist, Salesforce
03: Nathan Eagle, CEO, Jana Mobile
04: Omer Laviv, CEO, Athena Security Implementation
05: Vic Mankotia, Senior Vice-President, Corporate Strategy and Solution Sales, CA Technologies
06: Naveen Menon, Partner, AT Kearney

03

06

Delivering on Digital Infrastructure

Key Issues

- What should be the adequate investments in digital infrastructure?
- Who are the key stakeholders in the digital infrastructure dialogue?
- What are the right regulatory frameworks of the digital infrastructure?
- What should be the new business models to fund the investments to satisfy customers' need for value and service delivery?

Synopsis

The promise of the digital economy has never looked brighter. Consumers and businesses love the Internet and use more of it, in more places, every day. The increased use of smart phones and tablets, coupled with high-speed fixed networks, is driving Internet traffic exponentially higher, with one participant predicting usage levels in 2020 a thousand times higher than today. Bandwidth-intensive activities like gaming, video streaming, education delivery and healthcare remote monitoring are becoming routine actions on mobile devices and contribute strongly to this growth. All of this demand for connectivity and digital services is leading to far greater demands on the digital infrastructure that underlies this emerging digital economy.

Significant investments in fixed and mobile networks as well as cloud infrastructure will be required to provide the necessary capacity and bandwidth. However, concerns about their ability to earn adequate returns have caused many telecommunications operators to reduce their investments in network rollout.

The tension between high customer demand and limited economic returns for some set the stage for a lively debate among participants. Telecommunications operators highlighted the magnitude of investments required, while others insisted alternative infrastructure models with smaller and smarter investments represented better solutions to this impasse. Several participants believed a new approach to spectrum allocation was necessary to encourage greater utilization and direct more investments towards physical infrastructure. Others pointed out the importance of licensed spectrum in ensuring quality of service for consumers and helping operators earn returns on their infrastructure investments. Finally, there was debate about who should pay for improvements in infrastructure. In the current value chain, telecommunications operators are making major investments in capacity that enable the business models for digital services players. However, digital services players are also making large investments – in cloud infrastructure and R&D on new devices and services.

01: Participants of the Delivering on Digital Infrastructure
02: David Tennenhouse, Corporate Vice-President, Technology Policy, Microsoft

While resolution to specific issues remains unclear, there was agreement on the need to modernize the regulatory framework to support infrastructure investment. Fixed and wireless connectivity services are converging, as are communication and entertainment services.

Likewise, digital services are by nature international. Regulatory bodies of the future must recognize the converging and inherently international nature of these industries. Moreover, without international cooperation, the world runs the risk of a Balkanized Internet, where some countries decide to go their own way. Industry stakeholders could find themselves unable to take advantage of the full scale of the Internet and end users could find themselves with a more limited selection of services.

Today, many future scenarios for digital infrastructure are possible, and the path rests on the decisions of policy-makers and industry participants. A best-case scenario would feature high consumer demand and willingness to pay for connectivity and digital services. Regulations would be as light as possible, primarily guaranteeing universal access. Optimism would guide infrastructure providers to make smart, ample investments ahead of demand. In the worst-case scenario, consumer demand for digital services could fall if prices rise while quality of service for infrastructure decreases. This scenario could come about if infrastructure providers do not invest or governments fail in their basic regulatory roles.

Alternatively, the digital infrastructure landscape could look radically different from current industry norms in the next three to five years. New partnerships and business models that redefine the value chain are all possible, and may actually represent the most efficient solutions for providing availability and innovation in digital infrastructure.

Despite the uncertainty, there was a high degree of optimism that challenges would be overcome. This success will require new levels of cooperation between stakeholders, and potentially a new value chain that funds and rewards investment challenges very differently than today. Government policy-makers and regulators must recognize that technology often moves faster than regulation does, and should avoid the possibility of bottlenecks. A light touch that recognizes the converging and international nature of the Internet is required to address the demands of the future.

01: Participants of the Delivering on Digital Infrastructure
02: Ken Hu, Deputy Chairman, Huawei Technologies
03: David Kirkpatrick, CEO, Techonomy Media
04: Participants of the Delivering on Digital Infrastructure
05: Larry Stone, President, Group Public and Government Affairs, BT

Protecting the Digital Economy

(official programme session)

Key Issues

- Central to cybersecurity is the need for trust and transparency.
- Cybercrime is transnational and transborder, which means cooperation among all stakeholders is critical.
- An international regulatory framework is needed.
- A shared understanding of risk is essential to cooperation.

Synopsis

News on all fronts over the past year has stepped up the public debate about cybersecurity – protecting individual, national and global security and privacy. A leitmotif of the debate is the need for trust and transparency in today's increasingly hyperconnected world.

Panellists discussed the inextricable linkages between privacy and security, and noted that tension between the two tends to paralyse governments. However, the private sector appears to opt for the technological solution for security if privacy is not compromised. The Minister of Communication and Information Technologies of Azerbaijan joined panellists in calling for an international regulatory framework for cybersecurity. But policy-makers are still grappling with the tension at a national level. Cyber-risks abound, particularly in the financial services sector. For Chris Clark, Group Executive, Asia-Pacific, Visa, Hong Kong, cybersecurity is fundamental to his company's business model. He described a system of shared responsibility through different levels of protection.

A shared, more sophisticated understanding of risk is needed, according to Kevin Mahaffey, Chief Technology Officer and Co-Founder, Lookout Mobile Security, USA. Currently, there is no way for service providers, the private sector and governments to exchange information. "It is very ad hoc".

Vic Mankotia, Senior Vice-President, Corporate Strategy and Solution Sales, CA Technologies, Singapore, said that the digital economy will thrive in a "trustful" environment. "Industry is getting a second chance to earn trust back. The right people with the right access to the system with the right device helps to build an ecosystem of trust," he said. "Technology and the evolution of the digital economy will be faster than the legislation. The genie is out of the bottle. There is no perfect way. We need a paradigm and mind shift."

China experienced a serious cyber-attack last August when the country code top-level domain for Mainland China was hacked. "[This was] the first time hackers attacked a national system directly. We need very close cooperation between government, industry, service providers and NGOs… I have a dream that in the future we will have a trustworthy network," said Lee Xiaodong, Chief Executive Officer, China Internet Network Information Center, People's Republic of China. "To build trust, network law enforcement is very important… and very important for governance." Protecting infrastructure is the government's job, most panellists agreed.

01: Panelists in the Protecting the Digital Economy

To do this, partnering with Internet service providers (ISPs) and other private sector actors is the way forward. Another area for fruitful cooperation is risk management. The private sector has taken the lead in this and often comes to government with solutions. In India, for example, it was not against the law for hackers to attack a non-government website. Clark and his team worked with the government to change the law.

Industry often takes the lead in the privacy-security nexus. “We want to create a world where security enables countries to trust and share,” added Mahaffey. “When there is no trade-off between privacy and security, we should take the technological solution that provides security.”

In response to a question from the audience concerning transparency, panellists noted that it is essential, but at the same time people’s data must be secure and protected. People have the right to know the process, who is involved and the duties of ISPs and governments. One solution to this dilemma is already being provided by the private sector. Mahaffey noted that a “good check and balance” is the trend for companies to provide reports when they are asked to provide data.


01


02


03

04

01: Xiaodong Lee, CEO, China Internet Network Information Center
02: Chris Clark, Group Executive, Asia Pacific, Visa
03: Kevin Mahaffey, Chief Technology Officer, Lookout Mobile Security
04: Gady Epstein, China Correspondent, The Economist and Ali Abbasov, Minister of ICT, Azerbaijan

Strategic Shifts in the Digital Ecosystem

(official programme session)

Key Issues

- The move from fixed digital devices to mobile is one of the biggest shifts in the digital ecosystem.
- The new digital ecosystem is connecting both people and objects.
- Changes in the digital world will force us to re-examine how we deal with issues such as unemployment, data protection and organizational structures.

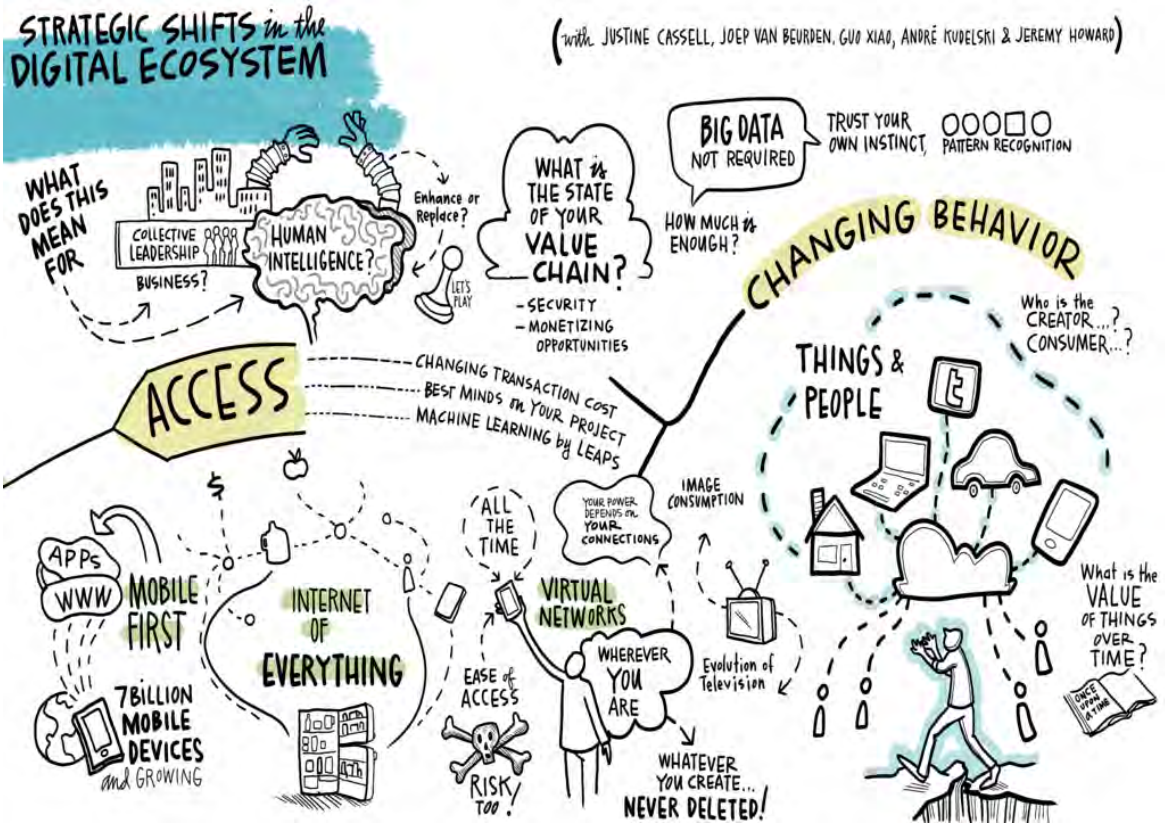
Synopsis

From the individual to the collective, from fixed to mobile, from the private to the public, the digital ecosystem is evolving faster than our societies, institutions and organizations can keep up. As individuals operate in the digital world, the distinction between the creation, ownership and consumption of data is becoming muddied. There is value in understanding how individuals interact within the digital ecosystem and how those interactions combine. The biggest shift in the digital ecosystem is the permanent and ongoing move from fixed digital devices to mobile. As a result, investment in landline infrastructure is declining and mobile technology is becoming central to the strategies of all players in the digital world. Despite the growth of the Internet globally, some 80% of Web traffic continues to go through the United States.

The Internet is becoming more than a network of information nodes; it is becoming the "Internet of Everything". With 7 billion smart devices, the Internet of Everything connects the milk in your refrigerator to the cow needed to produce it.

As a result of the mobile revolution, reaction times have radically shortened. It means everyone from content producers to hardware makers needs to adapt at a remarkable speed. Today, most content is streamed using mobile devices, relegating the "thing" – in this case the TV – to the status of display screen. As the changes provide more opportunities for hackers and data thieves, individuals need to think about what parts of their lives they are willing to share and what is special to them.

With some 30% of the global population online, there are enormous opportunities to bring together people to resolve complex problems. This means that artificial computing is being left behind by the sheer power of human computing. Together, the collectivization of brains, the power of machine learning and aggregated computing could lead to breakthrough ideas and solutions. The changing digital ecosystem is also having an impact on the world of work. According to one panellist, we are moving into a new era where there will be a permanent and significant shift in the unemployment level, as technology makes things easier and quicker to do. Productivity will be such that there will be a swathe of the permanently unemployed.



Collective leadership that leverages the intellect of the world will be part of the solution. As more ways to extract and understand data emerge, companies need to have clearly defined strategies for monetizing that data. Strategic shifts in the digital ecosystem are being determined by the embedding of artificial intelligence and data tracking into almost everything we do. Every time people search for something on Google, they are being assisted by artificial intelligence. When people update their status on Facebook, they are contributing to the data stream. The combination of immense amounts of information and the collective ability to interpret it and act on the results is influencing our future in exciting and terrifying ways.

Addressing the Digital Divide

(official programme session)

With access to employment, institutions and markets increasingly reliant on digital infrastructure, how can the growing digital divide be addressed?

Dimensions addressed:

- Skills training for the knowledge economy
- Participating in a civic dialogue
- Fostering entrepreneurship and employment

Acknowledgements

We would like to thank our partners for sharing their insights and for contributing to the ICT Industry program at the Annual Meeting of the New Champions.

Andrew	Jim	Executive Vice-President; Chief Strategy and Innovation Officer; Chairman, Sustainability Board; Member, Executive Committee, Royal Philips
Antonovich	Michael D.	Supervisor, Los Angeles County
Ayala	Orlando	Chairman, Emerging Markets, Microsoft Corporation
Boudrias	Claude	Director, Global Government Relations, CA Technologies
Brooks	Stuart	Special Adviser, Chevron
Byrne	Gerard	Chief Operating Officer, APAC, Middle East, Africa and Turkey, BT
Chandrasekher	Anand	Senior Vice-President and Chief Marketing Officer, Qualcomm
Cross	Stephen	Executive Vice-President for Research, Georgia Institute of Technology
David	Scott	Executive Director, Law, Technology and Arts Group, University of Washington
Eckelmann	Robert	Chairman of the Advisory Board, Midis Group
Egloff	Gaetan	Chief Digital Officer; Managing Director, Vietnam Lab, WISeKey
Esparza	Alfredo	Director, Strategy and Business Intelligence, Grupo Lauman
Fabela II	Augie K.	Co-Founder and Chairman Emeritus, VimpelCom
Felton	Nicholas	Data Visualizer, The Office of Feltron
Frazier	Tony	Senior Vice-President, Marketing and Insight, DigitalGlobe Inc.
Gardiner	Will	Chief Financial Officer, CSR
Grob	Matthew	Executive Vice-President and Chief Technology Officer, Qualcomm
Guo	Xiao	Chief Executive Officer, ThoughtWorks
Gupta	Sandeep	Chief Technology Officer, Microsoft Corporation
Held	Lindsey	Vice-President, Global Government Relations, SAP
Howlin	Brendan	Minister of Public Expenditure and Reform of Ireland
Hu	Ken	Deputy Chairman, Huawei Technologies
Iashvili	Giorgi	President, Black and Caspian Seas IT Association
Kirkpatrick	David	Founder, Chief Executive Officer and Chief Techonomist, Techonomy Media
Kudelski	André	Chairman of the Board and Chief Executive Officer, Kudelski Group
Laviv	Omer	Chief Executive Officer, Athena Security Implementations Ltd
Lee	Xiaodong	Chief Executive Officer, China Internet Network Information Center

Mahaffey	Kevin	Chief Technology Officer and Co-Founder, Lookout Mobile Security
Mankotia	Vic	Senior Vice-President, Corporate Strategy and Solution Sales, CA Technologies
Mittal	Vineet	Co-Founder and Managing Director, Welspun Energy
Mondini	Christopher	Vice-President, Business Engagement, Internet Corporation for Assigned Names and Numbers
Moran	Jane	Global Chief Information Officer, Thomson Reuters
Mukai	Hiroyuki	Senior Executive Managing Director, transcosmos Inc.
Nicolas	Christophe	Senior Vice-President; Head, Kudelski Security, Kudelski Group
Peralta Sanchez	José Ignacio	Undersecretary of Communications of Mexico
Pointer	Susan	Senior Director, Public Policy and Government Relations, Google
Rangaswami	JP	Chief Scientist, Salesforce
Reddy	Srikar	Managing Director and Chief Executive Officer, Sonata Software
Rierson	Brett	Director, China Office, United Nations World Food Programme
Rohner	Hugo	Chief Executive Officer, Skidata - Kudelski Group
Schwartz	Peter	Senior Vice-President, Global Government Relations and Strategic Planning, Salesforce
Sims	Zach	Chief Executive Officer and Co-Founder, Codecademy
Smith	Douglas	Assistant Secretary for the Private Sector, US Department of Homeland Security
Sonmez	Murat	Executive Vice-President, Global Field Operations, TIBCO Software
Stone	Larry	President, Group Public and Government Affairs, BT Group
Sullivan	Jay	Chief Operating Officer, Mozilla Corporation
Tennenhouse	David	Corporate Vice-President, Technology Policy Group, Microsoft Corporation
Van Riek	Maurice	Senior Vice-President, Head of Content and Asset Security, Kudelski Group
Viana	Antonio	Executive Vice-President, Commercial and Global Development, ARM
Wakileh	Michael	Chief Executive Officer, ProgressSoft Corporation
Wang	David	President, Government Affairs, Huawei Technologies
Wang	Xiang	Senior Vice-President and President, Greater China, Qualcomm China
Wang Yongfeng		President, Neusoft Corporation
Wu	Allen	President, Greater China, ARM Consulting (Shanghai) Co.
Yu Chuang Kuek		Vice-President, Asia, Internet Corporation for Assigned Names and Numbers
Yuzaki	Hidehiko	Governor of Hiroshima Prefecture
Zanuso	Silvano	Global Head, Scientific Research and Development, Technogym SPA

ICT Industry Team

Alan Marcus
Senior Director, Information Technology and Telecommunications Industries
alan.marcus@weforum.org

Aurelie Corre
Team Coordinator, Telecommunications Industry
aurelie.corre@weforum.org

John Corwin
Project Manager, Delivering on Digital Infrastructure
john.corwin@weforum.org

William Hoffman
Associate Director, Head of Rethinking of Personal Data
william.hoffman@weforum.org

Danil Kerimi
Director, Government Community, Information Technology Industry danil.kerimi@weforum.org

Elena Kvochko
Manager, IT Industry, Partnership for Cyber Resilience
elena.kvochko@weforum.org

Derek O'Halloran
Associate Director
Head of the IT Industry
derek.ohalloran@weforum.org

Justin Shepherd
Project Manager, The New Data Commons
justin.shepherd@weforum.org

Roshan Vora
Project Manager
Risk and Responsibility in a Hyperconnected World
roshan.vora@weforum.org

Bruce Weinelt
Director, Head of Telecommunications Industry
bruce.weinelt@weforum.org

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum is an independent international organization committed to improving the state of the world by engaging business, political, academic and other leaders of society to shape global, regional and industry agendas.

Incorporated as a not-for-profit foundation in 1971 and headquartered in Geneva, Switzerland, the Forum is tied to no political, partisan or national interests.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org