Welcome

9:00 a.m. – 9:15 a.m.

Welcome from AT&T
• Len Cali, Senior Vice President of Global Public Policy, AT&T

Welcome from USCIB:
• Peter Robinson, President, U.S. Council for International Business (USCIB)

Welcome from the OECD:
• Andrew Wyckoff, Director OECD Directorate for Science Technology and Innovation (STI)

Welcome from Business at OECD:
• Russel Mills, Secretary General, Business at OECD
Opening Remarks

9:15 a.m. – 9:25 a.m.

• Julie Brill, Corporate Vice President and Deputy General Counsel, Microsoft Corporation and Co-Chair, Business at OECD Committee on Digital Economy Policy (CDEP)
Modernizing Privacy & Security As The World Goes Digital

Julie Brill
Corporate Vice President & Deputy General Counsel
Global Privacy & Regulatory Affairs
Microsoft
GOING DIGITAL
Making the transformation work for growth and well-being

- Access
- Use
- Innovation
- Jobs
- Society
- Market Openness

Growth & Well-being
The world has been transformed
Artificial Intelligence for good
“Right to be let alone.”
—Louis Brandeis
Artificial Intelligence in our lives
“Ultimately the question is not what computers can do. It’s what they should do.”
Microsoft’s commitment to GDPR, privacy and putting customers in control of their own data

May 21, 2018 | Julie Brill - Corporate Vice President and Deputy General Counsel, Microsoft

That’s why today we are announcing that we will extend the rights that are at the heart of GDPR to all of our consumer customers worldwide. Known as Data Subject Rights, they include the right to know what data we collect about you, to correct that data, to delete it and even take it somewhere else. Our privacy dashboard gives users the tools they need to take control of their data.
Washington Senate approves consumer-privacy bill to place restrictions on facial recognition

Originally published March 6, 2019 at 6:33 pm | Updated March 7, 2019 at 1:15 pm

Senate Bill 5376 would allow citizens to know what information data companies — from big corporations like Facebook and Microsoft to behind-the-scenes data-collectors — are gathering.

OLYMPIA — In a broad bipartisan vote, Washington state senators have approved a bill to create a European-style consumer-data privacy law and restrict some uses of facial recognition.

Lawmakers on Wednesday voted 46 to 1 to pass Senate Bill 5376. Sponsored by Sen. Reuven Carlyle, D-Seattle, it would allow citizens to know what information data companies are gathering on them.

Those corporations could range from global behemoths, like Facebook and Microsoft, to retail stores and largely invisible data brokers.
Core elements of a modern, robust privacy law

- Transparency through meaningful disclosures
- Individual empowerment that grants people meaningful control
- Corporate responsibility weighing benefits and risks
- Robust enforcement and rulemaking
Keynote Address

9:25 a.m. – 10:00 a.m.

• Adam Lusin, Director, International Communications, Information, and Emerging Technologies, U.S. Department of State
Conference Prologue

Going Digital: Making the Transformation Work for Growth and Well-Being

10:05 a.m. – 10:30 a.m.

OECD Speaker:

• Andrew Wyckoff, Director OECD Directorate for Science Technology and Innovation (STI)
The OECD Going Digital project

The motivation

• Help policy makers understand how digital transformation impacts the economy and society.

• Reduce the gap between technology and policy development.

• Provide policy makers with the tools needed to develop a whole-of-government approach.

• Advance the measurement of digital transformation.
An Integrated Policy Framework

Access

Market openness

Use

Growth and well-being

Trust

Innovation

Society

Jobs
Enhancing access

By 2022, three devices per person will be connected around the globe.

There are only 7 fibre subscriptions per 100 people across the OECD.

56% of rural households have access to fast fixed broadband, in comparison to over 85% of households in urban and other areas.

Access to data drives innovation, new products, organisational models and markets.

Prepare for a massive increase of connected people, devices and demand on networks.

Invest in broadband infrastructure, especially fibre, to unlock digital technologies’ potential.

Improve access in rural and remote areas to connect everyone and everything.

Enhance access to and sharing of data to unleash its potential, balancing benefits and risk.
Mobile data usage is growing fast in most countries

Average monthly mobile data usage per mobile broadband subscription, GB, 2017

What matters most for policy?

- Promote **competition** to drive investment.
- Ensure **technical enablers** are in place.
- Boost **connectivity** in rural and remote areas.
- Enhance **access to** and sharing of **data**.
Increasing effective use

74% of people use e-mail...

...more sophisticated activities, like online courses (9%), still have great potential to grow.

Great potential could be unleashed if more firms, especially SMEs, would perform big data analysis.

Boost diffusion of advanced digital tools, especially for SMEs, to drive productivity.

Less than 60% of people visit or interact with public authorities’ websites.

Design user-centred digital public services to enhance usage and inclusion.

31% of adults have sufficient problem-solving skills for technology-rich environments.

Invest in skills to empower everyone to thrive in the digital age.
Large potential remains for diffusion of digital tools among firms

Diffusion of selected digital tools among firms, by firm size, as a percentage of all firms, 2018

Increasing effective use

What matters most for policy?

• Empower everyone with a **mix of skills** to thrive and trust in a digital world.

• Boost **diffusion of digital tools** to drive productivity growth in firms, SMEs in particular.

• Shift from an e-government to a **user-driven digital government** approach.

• Address mistrust to increase **online engagement**.
Unleashing innovation

Almost one third of business R&D expenditure is in information industries.

Foster innovation through investment in R&D, especially in information industries.

AI start-ups attracted 12% of worldwide private equity investments in the first half of 2018, up from 3% in 2011.

Harness the potential of digital technologies for innovation and science.

Over 2013-16, about 33% of OECD countries’ patents were ICTs, compared to about 60% of China’s.

Stimulate digital innovation by investing in intangible assets, e.g. patents or software.

Open government data boost innovation in the public and private sectors.

Realise open government data’s potential to foster digital innovation.
Investment in intangible assets is key to unleash digital innovation

Investment in ICT equipment and intangible assets as a percentage of GDP, 2017

Data is the “new R&D” for 21st century innovation systems

- Public Administration
- Agriculture
- Health
- Retail
- Science and Education
- Transportation
What matters most for policy?

• Boost **entrepreneurship** by reducing regulatory burdens for start-ups.

• Incentivise investment in **basic R&D and intangible assets**.

• Foster **knowledge diffusion** through open innovation and open science initiatives.

• Encourage **policy experimentation** and new business models across sectors.
Ensuring good jobs for all

An estimated 14% of jobs face high likelihood of automation and another 32% are likely to face significant change in how they are carried out.

Many jobs are likely to change.

Support workers to facilitate their transition into jobs with a low likelihood of automation.

Despite high returns on training the low-skilled, firms provide more training to high-skilled workers.

40% Low skilled
73% High skilled

Workers receiving training

Step up and target training, especially for the low-skilled.

Over the past decade, 4 out of 10 new jobs in the OECD were created in highly digital-intensive sectors.

NEW JOBS

Highly digital-intensive sectors

Promote education and training to deliver a mix of skills to succeed in a digital world of work.

Only 0.13% of GDP on average is spent on training of the unemployed and of workers at risk of involuntary unemployment.

Ensure that nobody is left behind as labour markets transform.
Digital-intensive sectors contribute to job creation

Contributions to changes in total employment, by digital intensity of sectors 2006-16

Ensuring good jobs for all

What matters most for policy?

• Promote **successful and fair transitions** from declining to expanding jobs.

• Ensure people have **the mix of skills needed to succeed** in a digital world of work.

• Get ready for a massive **training** challenge and review **education** systems.

• Address concerns around **emerging forms of work** and improve **social protection**.
Promoting social prosperity

About **12%** of people post opinions on civic or political issues online.

Use digital technologies to increase civic and political engagement.

About **9%** of 15-year olds say they are subject to cyberbullying.

Balance the opportunities and risks of using digital applications for mental health.

**More than twice** as many young men than women are able to program.

Address digital divides, e.g. by gender, age and level of education.

Digital technologies can help tackle key domestic and international issues, e.g. improve environmental protection and health care for all.

Harness the potential of digital technologies to address great societal challenges.
More young men than women can program

Share of 16-24 year-olds who can program, as a percentage of all Internet users, 2017

What matters most for policy?

• Boost **civic engagement** through digital government strategies and involve all stakeholders.

• Reduce **digital divides** by strengthening foundational skills and lifelong learning to include everyone.

• Harness the potential of digital technologies and data to address **collective challenges**.
Strengthening trust

Almost 30% of Internet users mistrust social and professional networks.

Address digital security, privacy and consumer protection concerns to improve trust.

One in four Internet users in the European Union is concerned about payment security.

Empower everyone to assess and better manage digital security risk.

Only 17% of peer platform users read terms and conditions in full.

A majority of privacy measures aims to raise awareness and empower individuals.

Design and implement more effective measures to protect consumers online.

Develop and implement a national privacy strategy with a whole-of-society perspective.
Strengthening trust

Payment security and privacy concerns remain prevalent

Individuals who did not buy online for payment security or privacy concerns, as a share of Internet users, 2017

Strengthening trust

What matters most for policy?

• Use **risk management** as a framework to develop policies to increase trust.

• Develop and implement a **national privacy strategy** with a whole-of-society perspective.

• Support **consumers** in facing challenges in digital environments.
Fostering market openness

Firms in the most digital-intensive sectors enjoy a 55% higher mark-up than firms in less digital-intensive sectors.

Strengthen competition for firms in all sectors to benefit from digital opportunities.

Digitally deliverable services make up about a quarter of total services trade.

Total services trade

23% Imports

28% Digitally deliverable

Encourage the spread of digital technologies and cross-border data flows to boost trade.

45% of EU firms undertook cross-border e-commerce sales in 2016, up from 42% in 2010.

Facilitate cross-border e-commerce to push out the trade frontier.

Cross-border acquisitions of digital-intensive firms grew by 20 percentage points more than those in other sectors over 2007-15.

Mergers & acquisitions

Consider industry concentration when reviewing M&As, especially of digital-intensive firms.
Measures restricting trade in services that enable digital delivery are primarily related to infrastructure and connectivity

OECD Digital Services Trade Restrictiveness Index, 2018

Industry concentration is increasing across regions

Industry concentration in Europe & North America, 2000-2014

Share of the top 4 firms (CR4) or the top 8 firms (CR8) sales in Europe

![Graph showing the share of the top 4 firms (CR4) or the top 8 firms (CR8) sales in Europe from 2000 to 2013.]

Share of the top 4 firms (CR4) or the top 8 firms (CR8) sales North America

![Graph showing the share of the top 4 firms (CR4) or the top 8 firms (CR8) sales in North America from 2000 to 2013.]

Note: The countries for Europe include BE, DE, DK, EE, ES, FI, FR, GB, GR, HU, HR, IE, IS, IT, LV, NL, NO, PL, PT, RO, SI, SE, and for North America include CA and US. Included industries cover 2-digit manufacturing and non-financial market services. Concentration metrics are the share of the top 4 firms (CR4) or the top 8 firms (CR8) sales. The top firms are defined as the 4 or 8 firms with the largest sales in each year. The reported figures in each industry in the total industry correspond to averages across all industries in each region and year. The measures capture concentration within the respective global regions (Europe, North America), not within individual countries.

Source: Bagjar et al, forthcoming.
Enormous growth in M&As of Information Services

Value of M&As in Digital Sectors – Normalised (2005 = 100)

Sectors are defined by the industry of the target company.
Fostering market openness

What matters most for policy?

• Monitor changing **competitive dynamics**, especially trends in market concentration and dominance.

• Lower **trade barriers** and ensure holistic market openness policies.

• Reduce **barriers to international investment**, including in communications infrastructures.

• Ensure that **tax systems** are fit-for-purpose in the digital age.
The Going Digital Toolkit

[Diagram with categories: Access, Growth & Well-being, Innovation, Society, Jobs, Use, Market Openness]

toolkit

www.oecd.org/going-digital-toolkit
#GoingDigital
THANK YOU!

https://doi.org/10.1787/9789264312012-en

https://doi.org/10.1787/9789264311992-en

Going Digital Toolkit:

Andrew.Wyckoff@oecd.org
Break

THE JOSEPH H. ALHADEFF DIGITAL ECONOMY CONFERENCE SERIES PRESENTS:

Going Digital: OECD Insights for a Changing World

March 25, 2019
Washington D.C.
Going Digital’s Policy Recommendations: From Paper to Practice
11:00 a.m. – 12:15 p.m.

Moderator:
• Ellen Blackler, Vice President, Policy Strategy, Global Public Policy, The Walt Disney Company and Vice-Chair, Business at OECD Committee CDEP

Panelists:
• Rory MacFarquhar, Director for Global Economic Policy, Google
• Molly Lesher, OECD Secretariat, Going Digital Project
• Rich Clarke, Assistant Vice President, Economic and Regulatory Policy, Global Public Policy, AT&T
• Adam Murray, International Relations Officer, Office of International Communications and Information Policy, U.S. Department of State
Going Digital Toolkit

THE JOSEPH H. ALHADEFF
DIGITAL ECONOMY CONFERENCE
SERIES PRESENTS:

Going Digital:
OECD Insights for a Changing World

March 25, 2019
Washington D.C.
Three entry points

Discover and explore the Going Digital Toolkit in three ways

Policy dimensions

Countries

Themes
Policy Dimension Pages

The Going Digital Toolkit allows users to assess performance in each dimension of the Going Digital Integrated Policy Framework. For example, the Use policy dimension includes indicators of how people and firms use digital technologies by country. Related publications and policy guidance are also provided to help design and develop well-suited policies.

- Indicators
- Related publications
- Policy guidance
Reference & country values

- OECD
- EU28
- OECD countries
- BRIICS countries
- Accession countries

- OECD countries
- BRIICS countries
- Accession countries
Explore by Themes

Digital transformation cuts across many aspects of the economy and society. Explore transversal themes and related OECD analysis and indicators.

- Data and data flows
- Development
- Digital government
- Digital technologies
- Gender
- Productivity
- Skills
- SMEs
Explore the Toolkit

The Going Digital Toolkit includes indicators, policy guidance and related publications to help countries realise the promises of digital transformation.

www.oecd.org/going-digital-toolkit
#GoingDigital
Going Digital’s Policy Recommendations: From Paper to Practice

THE JOSEPH H. ALHADEFF DIGITAL ECONOMY CONFERENCE SERIES PRESENTS:

Going Digital: OECD Insights for a Changing World

March 25, 2019
Washington D.C.
Connectivity is key to the digital transformation – but is generally being addressed satisfactorily in the OECD countries:

- 70% to 90% of all households subscribe to fixed broadband
- 92% of business enterprises also have broadband subscriptions
- Mobile broadband networks and take-up are practically ubiquitous
But connectivity challenges remain

- Broadband availability in rural areas is lower than in urban areas and speeds are slower
- SME connections lag those of larger enterprises
- Customers tend to choose basic connections even when more advanced connections are available
- Network availability, quality and take-up is generally lower in non-OECD countries
The Report is largely on point as to policies that will promote enhanced access:

- Incentivize further investment
- Increase spectrum allocations and reduce impediments to infrastructure deployment
- Increase digital literacy, diffusion of digital applications and trust to expand business and residence take-up and use of digital tools
• But in a few areas the policy recommendations are questionable or discordant
  – Role of fiber technologies over non-fiber technologies appears to be excessively elevated
  – Wholesale or sharing arrangements for both networks and data are lauded without substantial evidence of their efficacy
• Key to Phase 2 is refining policy recommendations based on expanded evidence and analysis
Conference Luncheon with Keynote Speaker

12:30 p.m.-2:00 p.m.

Introductions/Moderator:
• Tom Dailey, Senior Vice President and General Counsel, Verizon International

Speaker:
• David Redl, Assistant Secretary for Communications and Information and Administrator of the National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce
Session Two

Securing the Digital Economy from Cyber-Threats
2:00 p.m. – 3:30 p.m.

Moderator:
• Chris Boyer, Assistant Vice President of Global Public Policy, AT&T

Panelists:
• Laurent Bernat, OECD Secretariat, OECD Global Forum on Digital Security for Prosperity
• James D. Katavolos, Senior Vice President, Citigroup Cyber Intelligence Center
• Miguel Sánchez, Global Chief Security & Intelligence Officer (GCSIO), Telefonica
• Makoto Yokozawa, Senior Consultant, Nomura Research Institute and Co-Chair, Business at OECD CDEP
OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity

- International instrument developed through a multistakeholder process
- High-Level Principles on how to approach digital security from an economic and social perspective
- Guidance on national digital security strategies
- Companion document for further explanations of key concepts

https://oe.cd/dsrm
« Cybersecurity » is a multifaceted area.
Main challenge: ensuring security in an open & dynamic environment without inhibiting prosperity

Protecting activities in a closed environment

Protecting activities in an open, dynamic & global environment

Security prevails

Security serves prosperity
Key messages to organisations’ leaders and decision makers

• Digital security is an economic and social (i.e. not just technical or national security) issue

• Risk (i.e. uncertainty) cannot be eliminated from an open and dynamic environment, but it can be managed, i.e.:
  – Assessed and reduced to an acceptable level, transferred, taken or avoided (avoiding also the benefits)

• Digital security risk should be managed together with the opportunities, i.e. integrated into entreprise risk management

• Business (i.e. not technical) decision makers should be responsible for digital security risk management
  – But they should work in co-operation with technical experts
Principles

**General principles**
1. Awareness, Skills, Empowerment
2. **Responsibility**
3. Human rights & fundamental values
4. **Co-operation**

**Operational principles**
5. Risk assessment & treatment cycle
6. Security Measures
7. Innovation
8. Preparedness & continuity
National Strategies

• Should address digital security as an economic and social issue (trust agenda)
  – While taking a holistic, whole-of-society & multi-stakeholder approach (all sectors, actors)
  – Characteristics: whole-of-government co-ordination, flexible, technology neutral, coherent with other strategies

• Should promote digital security risk management, inc. through:
  – Creation of Computer Emergency Response Teams (CERTs)
  – Better security education and skills
  – Encouraging information exchange on risks
  – Improving market efficiency and fostering a digital security market
  – Creating conditions for SMEs to better manage digital security risk
  – International co-operation
  – Better metrics
  – ...
OECD Global Forum on Digital Security for Prosperity

• Launched in 2018 to gather an international & multistakeholder community of digital security experts

• Events on themes proposed by governments

• Inaugural event
  – took place on 13-14 December 2018 in Paris
  – focused on « Roles and responsibilities of stakeholders »

• Second event is planned for Q4 2019 in London, on “Encouraging a thriving, innovative cyber security industry”
Content and outcomes from the Inaugural Event

Part I – Digital Security Risk Governance in Organisations
   Session 1 – Changing the culture at the top and breaking corporate silos
   Session 2 – How can value chain partners Trust Each other’s digital security governance?
   Session 3 – “Active defence” : How Far can Businesses Go in Proactive Security?

Part II – Making Digital Technologies more Secure Throughout Their Lifecycle
   Session 4 – How to achieve Security by Design ?
   Session 5 – Maintaining Security once Technologies are on the Market
   Session 6 – Encouraging Responsible Disclosure of Vulnerabilities


Report from the event will be available in June.
THANK YOU

More information:

Recommendation on Digital Security Risk Management: https://oe.cd/dsr

OECD Global Forum on Digital Security for Prosperity: https://oe.cd/gfdsp

Contact: Laurent.bernat@oecd.org
Why « digital » and not « cyber » ?

- No international consensus on terminology
- « Cyber »
  - Separates the opportunities from the risk (there are no cyber opportunities)
  - Is connoted as national & international security, and law enforcement (cyberdefense, cyberwarfare, cybercommand, cybercrime, etc.)
  - Is sometimes used for everything (creating confusion)

- « Digital »
  - Allows to manage digital opportunities and risks together
Overview of risk management cycle

- Take
  - Security measures
    - Appropriate & commensurate to the risk
  - Innovation
    - Adapt the activity & the sec. measures
- Reduce to acceptable level
  - Preparedness
    - Resilience & continuity
- Transfer to third party
- Avoid
- End of Activity (or no digital in the activity)

Risk assessment
What is the level of risk to the activity, i.e. possible consequences of uncertainty on economic & social objectives?

Risk treatment
Can the risk be modified to be aligned with one’s acceptable level of risk?

Definition of the economic & social objective(s)

Design of the economic & social activity
New Technologies, New Challenges

New Threats

- **5G**
  Data traffic

- **IoT**
  Millions of devices connected

- **AI / Big Data**
  Manage all data information

- **Data**
  Security & Privacy

- **Blockchain**
  Adds a Trust layer to the operations
Digital Security Strategy

Who we are?

A Four Platforms’ Company

<table>
<thead>
<tr>
<th>1st platform</th>
<th>2nd platform</th>
<th>3rd platform</th>
<th>4th platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network CONNECTIVITY</td>
<td>IT &amp; SYSTEMS DIGITALIZATION</td>
<td>Products y services</td>
<td>Cognitive Intelligence BIG DATA - AI</td>
</tr>
</tbody>
</table>

Securing: Company assets
Protecting: Integrity /privacy of client data

From... ...To
Digital Security Strategy

How we do that?

Digital Security

- ANTICIPATE
- PREVENT
- RESPOND
- DETECT

Information Security
- Governance & Processes
- Transformation
- Security Architecture

Cyber Intelligence, CT Control & Response
- Cyber Intelligence
- Red Team
- CSIRT

3 Functions

4 Pillars
Co-operation

Commitment to Digital Transformation

Public sector / Governments

• Rules & Ethics guidelines (European Commission, Regionals)
• National Legislation/ Administrations
• National Critical Infrastructures
• Nationals Cyber Strategies
• Nationals CSIRT / CERTs

Private sector / Organisations

• GSMA – “Digital Declaration” (WEF)
• Telco Cybersecurity Alliance (Telefonica)
• Data Portability (EU Telcos)
• Cybersecurity Tech Accord (Microsoft – 90 Cias)
• Global CSIRT (Telefonica)
Digital Manifesto

A New Digital Deal
Towards a human-centric digitalization

FAIRNESS + NON DISCRIMINATION
INCLUSIVENESS
ACCOUNTABILITY
TRANSPARENCY + CHOICE
RESPONSIBILITY
EMPOWERING PEOPLE
DIGITAL SECURITY WRAP
SMART PUBLIC POLICIES
DIGITAL BILL OF RIGHTS

Find more: https://www.telefonica.com/digital-manifesto/
Securing Digital Economy

March 25, 2019, Washington DC

Dr. Makoto (Mac) Yokozawa
Kyoto University/Nomura Research Institute, Ltd.
OECD/BIAC Digital Co-Chair
Keidanren (Japan Business Federation) Global Strategy WG Chair
(1) Develop policy frameworks to utilise data
   A) Establish the next generation data governance framework

   • Promote international interoperability of risk-based security and privacy protection standards across jurisdictions so as to ensure the free flow of data, information, ideas and knowledge across borders, while respecting applicable legal frameworks for privacy, data protection, and intellectual property rights.

(2) Promote international cooperation in the field of cybersecurity

   • Voluntary and Risk Based
   • Harmonization and Simplification
   • Global Supply Chains and Standards (ISO)
   • Incentives
   • Information Sharing
   • Public Private Partnership
   • Education
Japan’s Overview of Cybersecurity Measures

Before Society 5.0
(Traditional supply chain)

- Parts Manufacture
- Assembler
- Integrator

Society 5.0
(Flexible and non-linear supply chain)

A Call for Reinforcement of Cybersecurity
To Realize Society 5.0

Approach
- Self-help
- Cooperation
- Govt. assistance
- Global links

Change awareness & secure resources

Change Awareness

- Improve awareness among all citizens
- Change awareness among top management

Develop frameworks as foundation

Govt. framework
- Integrate govt. measures
- Develop in-company frameworks
- Manage supply chains

Corporate framework
- Develop legal system & technical standards
- Establish cybersecurity norms

Legal system & norms
- R&D
- Social implementation

Japan Business Federation

Frameworks in APEC and OECD

- APEC Framework for Securing the Digital Economy (discussed since 2015)
  - still need to be approved by APEC... (after TEL59 SPSG, 2019)
  - MSH vs Multilateralism

- Principles
  - Awareness
  - Responsibility
  - Cooperation
  - Privacy (+ to OECD)
    - (- From OECD : Human rights and fundamental values)

The project initially aimed to develop the APEC Cybersecurity Framework, with a view to help APEC economies improve their understanding and awareness of work going on across the region and in relevant international bodies, promote discussions of best practices for addressing key issues on the topic and begin to identify common themes and frameworks in regional and global approaches to secure, safe and trustful Online environment.


  MINDFUL that governments, public and private organisations, as well as individuals share responsibility, based on their roles and the context, for managing digital security risk and for protecting the digital environment; and that co-operation is essential at domestic, regional and international levels.

- Business supports on OECD’s work and MSH is so essential because;
  - limitation exists in how far service providers can do without collaboration from users/customers
  - maturity and awareness is approaching to the next saturation level. We will need much more social cost (and risks) than ever in gaining just 1% improvement in awareness and readiness for individuals.
  - structural reform will be required in further improvement in culture of security
  - private sector wants to join collaborative awareness/readiness development including education and skill developments
  - Participation from non-member countries and stakeholders are equally important as members

(Mac Yokozawa’s talk at GFDSP, 2018)
Other Thoughts

• What is “Collaborative” Security?
  • ISOC Report in 2015
    https://www.internetsociety.org/collaborativesecurity/approach/

• What is “Participative” MSH?
  • Who is missing in current MSH?
  • “Paris Call” by Emmanuel Macron
  • “First, we must be more than multistakeholders, we must also be multidisciplinary.” António Guterres (UN Secretary-General) at IGF 2018

• What is “secure and free flow”?
  • Cyber security Law in China
  • ”Cyber Sovereignty”?
  • Where are Market Mechanisms and Democracy?

• What is “Collaborative” MSH in Cyberspace?
  • Education?
  • Responsibility?
  • Risk?
  • Youth protection?
Break
Session Three

Harnessing Artificial Intelligence (AI) for Economic and Social Prosperity
3:45 p.m. – 5:00 p.m.

Special Speaker:
• Lynne Parker, Assistant Director for Artificial Intelligence (AI), Office of Science and Technology, The White House

Moderator:
• Carolyn Nguyen, Director, Technology Policy, Microsoft Corporation

Panelists:
• Andrew Wyckoff, Director OECD Directorate for Science Technology and Innovation (STI)
• Daniel Castro, Vice President, Information Technology and Innovation Foundation
• Eleni Kyriakides, International Counsel, Electronic Privacy Information Center
• Craig Stephen, Head of R&D Labs, Oracle
• Jordan Zed, Director General, External and Trade Policy Branch, Innovation Science and Economic Development, Government of Canada
AI at the OECD (2016-19)

– G7 ICT Ministerial meeting in Japan (Apr 2016)

– OECD Conference “AI: Intelligent Machines, Smart Policies” (Oct 2017)

– Measurement and analytical work
– Report on AI in society
– Expert Group and draft Recommendation of the Council on AI
– AI Policy Observatory
September 2018 – February 2019

Mission: to scope principles to foster trust in and adoption of AI
- Foster consistency and complementarity of AI policy, technical and practical guidance across international public and private organisations: G20, G7, EU, UNESCO, ISO, IEEE etc.

Composition: multi-stakeholder and multi-disciplinary: 50+ experts;

Outcome: 5 principles for responsible stewardship of trustworthy AI, 4 recommendations for AI policies and 1 for international cooperation
15-16 March: discussion and approval by the Committee of a draft Recommendation of the OECD Council

April-May 2019: transmission to, and adoption by, the OECD Council at its upcoming Meeting at Ministerial Level (MCM) on 22-23 May 2019

July-December 2019: development of practical guidance (living resource) and report to the OECD Council
Principles for responsible stewardship of trustworthy AI
1.1. Inclusive growth, sustainable development and well-being
1.2. Human-centred values and fairness
1.3. Transparency and explainability
1.4. Robustness, security and safety
1.5. Accountability

National policies and international cooperation for trustworthy AI
2.1. Investing in AI research and development
2.2. Fostering a digital ecosystem for AI
2.3. Providing an enabling policy environment for AI
2.4. Building human capacity and preparing for labour transition
2.5. International cooperation
Common understanding of terms

- **AI system** is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy.

- **AI system lifecycle** includes i) ‘design, data and models’; ii) ‘verification and validation’; iii) ‘deployment’; and iv) ‘operation and monitoring’.

- **AI knowledge** refers to the skills and resources, such as (…) required to understand and participate in the AI system lifecycle.

- **AI actors** are those who play an active role in the AI system lifecycle, including organisations and individuals that deploy or operate AI.

- **AI stakeholders** encompass all organisations and individuals involved in, or affected by, AI systems, directly or indirectly. AI actors are a subset of stakeholders.
Measurement
Trends - investments in AI start-ups

Total estimated investments in AI start-ups (USD billion) (2011 to 2017 and first semester 2018)

By start-up location

First Semester 2018
- USD 18B
- USD 16B
- USD 14B
- USD 12B
- USD 10B
- USD 8B
- USD 6B
- USD 4B
- USD 2B
- USD B

Jan-Jun 2018
- USD 18B
- USD 16B
- USD 14B
- USD 12B
- USD 10B
- USD 8B
- USD 6B
- USD 4B
- USD 2B
- USD B
1. **Purpose**
   - Foster understanding of AI (present and near-term).
   - Map economic & social impacts of AI and policy issues.

2. **Structure**
   i. Technical landscape
   ii. Economic landscape
   iii. AI applications and use cases
   iv. Public policy considerations
   v. AI policy landscape
OECD AI Policy Observatory
An online clearinghouse for AI information, evidence and policy options

Core pillars:

- Characteristics
  - Multidisciplinary
  - Evidence-based
  - Multistakeholder
THANK YOU

Andrew Wyckoff, andrew.wyckoff@oecd.org
Anne Carblanc, anne.carblanc@oecd.org
Oracle AI
Transforming the Enterprise

Craig Stephen
Senior Vice President, R&D, Oracle Labs

March 25, 2019
Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing and pricing of any features or functionality described for Oracle’s products may change and remains at the sole discretion of Oracle Corporation.
Oracle: 40 Years of Leadership in Enterprise Data
CREATE TABLE SALES_EXTENDED
(
    PROD_ID NUMBER,
    CUST_ID NUMBER,
    TIME_ID VARCHAR2(30),
    CHANNEL_ID NUMBER,
    PROMO_ID NUMBER,
    QUANTITY_SOLD NUMBER(10,0),
    AMOUNT_SOLD NUMBER(10,2),
    GENDER VARCHAR2(1),
    CITY VARCHAR2(30),
    STATE_PROVINCE VARCHAR2(40),
    INCOME_LEVEL VARCHAR2(30)
);

-- Load data
MODEL-BASED NUCLEAR POWER PLANT MONITORING AND FAULT DETECTION: THEORETICAL FOUNDATIONS

Ralph M. Singer, Kenney C. Gross, James F. Hercoq, Ronald W. King, Stephan Wegerich

Argonne National Laboratory
Argonne, IL, USA and Idaho Falls, ID, USA

ABSTRACT - The theoretical basis and validation studies of a multi-level, model-based process monitoring and fault detection system is presented. Through use of a non-linear state estimation technique coupled with a multihypothesis-based statistical hypothesis test, it is possible to detect and identify sensor, component and process faults at extremely early times from changes in the stochastic characteristics of measured signals. Data from an experimental test reactor and a commercial PWR are used to demonstrate functional capabilities of the monitoring system.

KEY WORDS
State estimation, fault detection, hypothesis test, surveillance.

INTRODUCTION AND BACKGROUND

From their earliest conception, nuclear power plants have included monitoring and fault detection systems in part of their basic designs. However, in many cases these systems were of fairly elementary character and usually consisted of nothing more than upper and lower limits placed upon important sensor measurements that when exceeded would alert plant operators. Although this approach has proved to be reasonably successful, considerable advances in methods of signal and information processing have permitted the development of new techniques that not only are much more reliable and robust, but also provide additional functional capabilities such as on-line sensor validation, extremely early fault detection and identification, provision of "normal" sensors for replacement of failed sensors, diagnosis and prognosis of disturbances, fault tolerant component operation, insight into the plant operational state, etc., at Argonne National Laboratory, such methods were initially developed to address critical operational issues in the Experimental Breeder Reactor No. 3 Power Plant (such as loss of coolantable sensors and forced shutdowns due to increased pump speeds) [1] and then expanded for use in commercial power plants as well as many industrial processes. This paper will describe the theoretical basis of the resulting monitoring and fault detection system and summarize the supporting validation studies. A companion paper in this Conference [2] will present results obtained from an experimental monitoring program performed at a commercial reactor power station.

OVERVIEW OF APPROACH

Numerous objectives can be achieved to a modern process monitoring system, but perhaps one of the most important ones, at least in terms of reducing operational and maintenance costs is the following: to detect and identify sensor deterioration sufficiently early to avoid forced shutdowns and physical damage. In other words, would be highly desirable to be able to detect disturbances so that necessary repairs can be scheduled and performed at some convenient plant operational requirements. This objective immediately leads to the following two points: the detection of disturbances prior to changes in signal mean values (when mean value changes, physical damage has likely occurred and shutdowns may not be far off) and the minimization of both false and missed alarms (false alarms ultimately result in poor economic and missed alarms can permit continued damage and probable shutdowns).

Accordingly, the first indicators of abnormal operation of a piece of equipment usually appear as changes in the characteristics of the noise on sensors associated with this equipment, the monitoring method must utilize such information to detect and identify disturbances. To achieve this functionality, a model-based monitoring method must utilize a technique that not only has a high precision (to minimize sensor mismatch) but also be easily adaptable to the changing configuration and operational changes in the plant. In addition, the fault detection portion of the method must identify disturbances based upon changes in statistical characteristics of the signals as well as the mean value with probabilistic and false alarm probabilities. These are challenging requirements.
MODEL-BASED NUCLEAR POWER PLANT MONITORING AND FAULT DETECTION: THEORETICAL FOUNDATIONS

Ralph M. Singer, Kenny C. Gross, James P. Herzog, Ronald W. King, Stephan Wegerich

Argonne National Laboratory
Argonne, IL, USA and Idaho Falls, ID, USA

ABSTRACT - The theoretical basis and validation studies of a real-time, model-based process monitoring and fault detection system is presented. Through use of a non-linear state estimation technique coupled with a probabilistically-based statistical hypothesis test, it is possible to detect and identify sensor, component and process faults at extremely early times from changes in the stochastic characteristics of measured signals. Data from an experimental fast reactor and a commercial PWR are used to demonstrate functional capabilities of the monitoring system.

industrial processes. This paper will describe the theoretical basis of the resulting monitoring and fault detection system and summarize the supporting validation studies. A companion paper in this Conference [2] will present results obtained from an experimental monitoring program performed at a commercial nuclear power station.

OVERVIEW OF APPROACH

Numerous objectives can be ascribed to a modern
Oracle AI Strategy
Ready-to-Go, Ready-to-Build, Ready-to-Work

Applications:
• Adaptive Intelligent Apps
• Intelligent UX
• Conversational Agents
• Smart Data

AI Platform:
• Data Management
• Data Science & Analytics
• Application Development
• Cloud Infrastructure

Autonomous Database:
• Self-driving
• Self-securing
• Self-repairing
More Information

Oracle.com/ai

craig.stephen@oracle.com
Integrated Cloud
Applications & Platform Services
Canada’s AI Landscape

- Three established AI institutes in Edmonton, Toronto, and Montreal
  - Funded by the $125 million Pan-Canadian AI Strategy, delivered by the Canadian Institute for Advanced Research (CIFAR)
  - Focus on supporting leading AI research and enhancing capacity for talent attraction and development
- A strong AI ecosystem in Vancouver is rapidly coalescing around a critical mass of start-ups and commercial applications.
SUPERCLUSTERS AND AI IN ACTION

**PROTEIN INDUSTRIES**
PRAIRIE PROVINCES
- Employment: more than 4,500 over 10 yrs.
- GDP: more than $4.5 billion over 10 yrs.
- Participants: 100+

**DIGITAL TECHNOLOGY**
BRITISH COLUMBIA
- Employment: more than 13,500 over 10 yrs.
- GDP: more than $5 billion over 10 yrs.
- Participants: 270+

**SCALE AI**
QUEBEC
- Employment: more than 16,500 over 10 yrs.
- GDP: more than $16 billion over 10 yrs.
- Participants: 110+

**ADVANCED MANUFACTURING**
ONTARIO
- Employment: more than 13,500 over 10 yrs.
- GDP: more than $13.5 billion over 10 yrs.
- Participants: 130+
CANADA’S AI LEADERSHIP

AI – A LEADING THEME OF CANADA’S 2018 G7 PRESIDENCY
- March Innovation Ministers’ Statement
- June Leaders’ Summit Declaration
- December Multistakeholder Conference

SCALE.AI & AI ACROSS SUPERCLUSTERS

ESTABLISHMENT OF THE INTERNATIONAL PANEL ON AI

D9 APPROACH FOR THE RESPONSIBLE USE OF AI BY GOVERNMENTS

PAN-CANADIAN AI STRATEGY
Announced by Prime Minister Trudeau and President Macron on June 7, 2018, Canada and France are working toward the establishment of an international body on artificial intelligence. The mandate for the International Panel on Artificial Intelligence (IPAI) was presented on December 6 by Canada’s Prime Minister and Minister of Innovation, Science and Economic Development and France’s Secretary of State for Digital Affairs.

“Canada and France are seeking to create an International Panel on AI that can become a global point of reference for understanding and sharing research results on AI issues and best practices, as well as convening international AI initiatives.”

– Mandate for the International Panel on Artificial Intelligence
MANDATE OF THE INTERNATIONAL PANEL ON ARTIFICIAL INTELLIGENCE

• To support and guide the responsible adoption of artificial intelligence that is human-centric and grounded in human rights, inclusion, diversity, innovation and economic growth.

• To facilitate international collaboration in a multistakeholder manner with the scientific community, industry, civil society, related international organizations, and governments.

• Monitor and draw on work being done domestically and internationally to identify gaps, maximise coordination, and facilitate international collaboration.

• Multidisciplinary analysis, foresight, coordination and policy development in the area of artificial intelligence.
Closing Session

Summary and Final Question & Answer
5:00 p.m.-5:30 p.m.

Post-Conference Reception
5:30 p.m.-7:00 p.m.