



**PEOPLE-
CENTERED**
INTERNET

Can Internet of Things be of the People, by the People, & for the People ?

Mei Lin Fung, *early CRM Pioneer with Tom Siebel, Marc Benioff*
Chair, People-Centered Internet *co-founded with Vint Cerf*

Chair, **IEEE Technical Committee, Sustainability, Society for the Social Implications of Technology**

Co-chair, **UN Women Commission on the Status of Women: Expert Roundtable for Asia Pacific, Africa, Europe, Middle-East) 2023 1st Report on Digital Innovation**

Lead author Japan G7 Presidency Think7 policy brief **People-Centered Science and Digital Transformation: A Practical Proposal for G7 & G20**

Led the People Centered Internet team who contributed to 11 of 70 policy papers for 2022 German G7 Presidency

Worked at Oracle (5y), Intel (5y), Shell (3y), US DoD (4 years, last 2y as Socio-Technical Lead for the Federal Health Futures Initiative)

Fellow of Hasso Plattner Institute, Berlin, Germany

3 Barriers to Global IoT Adoption

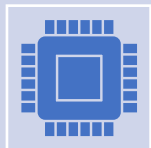


Security and Privacy

No assurance of Responsibility by Maker or Operator



Specific Devices have no unique identity, trackable through its lifecycle



Expensive custom devices inhibit widespread use and increasing functionality; *Lack of standards increase upfront and operating cost*

Internet of Things is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people, provided with **unique identifiers and the ability to transfer data over a network**

without requiring

- human-to-human or
- human-to-computer interaction.

LLII

IoT

Agenda

1. License
2. Label
3. Identity
4. Inter-operability

Responsible Tech Checklist For **Labeling**

centered on the person or people;

respectful of the natural environment and stewardship of the planet;

sustainable by design;

preserves desired privacy and security by design;

protects personal information with timely, specific informed consent on the private or public use of data;

accountable to the people who use it and to the planet —in addition to the people who fund and manage it;

ethical by the IEEE Code of Ethics;

deployed in solutions that are appropriate to the context of the problem (not all problems need technology);

deployed where a human is in the loop with respect to overseeing and managing technological systems; and

developed with due respect for justice, fairness, the law, and public interest.



IEEE SA STANDARDS
ASSOCIATION

IEEE Planet Positive Guiding Principles ([link](#))

People consume technology 24/7, and it affects our health and lives.

Keep Improving the design, development, use, and disposal of technology as an iterative, cyclic Dynamic Process



PCI: Voice-Enabled Conversational AI



Licensing and Labeling at Internet Speed and Scale

Adaptive IoT Licensing & Labeling allows for evolving appropriate, timely response at each stage of each IoT device's lifecycle

Feedback by designers, developers, public interest advocates, & citizens can identify harms & unforeseen consequences

IEEE Planet Positive Guiding Principles ([link](#))

License & Label IoT



Each wave of technology has unforeseen consequences: fire, language, writing, printing, electricity, transistors, AI, IoT...

We can learn from drug and nutrition labeling, which recognized the need to alert people about how they are affected by what they consume.



Design, development, use, and disposal of technology is a dynamic ongoing process. Licensing can allow for evolving appropriate, timely response to

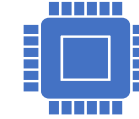
negative impacts—unforeseen consequences of technology on people and planet

positive impacts—opportunities to relieve suffering, increase flourishing and equity, and achieve the UN SDG Goals



Advanced technologies will not lead to nor generate beneficial outcomes automatically

for technology is only as good as we are



It is up to those of us who are technologists to decide

how technology is designed and developed

&

whether we believe that our technologies are being built to work and serve in the best interests of humanity.



IEEE Planet Positive Guiding Principles ([link](#))

Labeling - U.S. Cyber Trust Mark

BRAVO !

- Cybersecurity labeling program for internet-connected devices to be launched by 2024 ([link](#))

- **White House and Federal Communications Commission (FCC)**

Participation from several major retailers, including Amazon, Best Buy, Google, Logitech, and Samsung.

The program draws on voluntary commitments from manufacturers who have agreed to a certification program based on a set of cybersecurity criteria developed by the **National Institute of Standards and Technology (NIST)**, including “unique and strong default passwords, data protection, software updates, and incident detection capabilities.”

Manufacturers who agree to certification would be able to use a shield logo label on their products, signaling to consumers they have agreed to the NIST standards. The program will be administered by the FCC, with support from the Cybersecurity and Infrastructure Security Agency (CISA).

Regulators including the Department of Justice will designate oversight and enforcement standards.



Recommends
Digital Common Law

Recommends:
Participation &
Feedback Process
Iterative
Improvement

Technology Labeling



IEEE Planet Positive Guiding Principles ([link](#))

1. Responsible and ethical leadership from individuals, organizations, and communities - *Leadership requires collaboration and cooperation with all stakeholders impacted by decisions*
2. Justice, diversity, equity, and inclusion
3. Energy systems transformation
4. Mitigation and adaptation
5. The regenerative imperative and a circular economy
6. Balance between today's needs and the needs of the future
7. Alignment of global goals with local goals and actions
8. Culture of sustainability
9. **Responsible use of technology and technology labeling**
10. Knowledge-based decisions, transparency, and accountability



Get and Track feedback throughout the lifecycle of a device at clear checkpoints

- track and measure deployment of technology *at the innovation and experimentation stage*
- implement a **standardized feedback process** for innovation with **checkpoints** to catch *dangerous or irreconcilable issues, unforeseen consequences*
- **‘responsible technology’ labels** for robustly tested technology so *buyers are informed*
- **certification** of responsible technology in use *”by whom” and “for what purpose” so users know*
- **certification** of responsible disposal of technology *when End of Life is reached*

Above is from the IEEE Planet Positive Report: [link](#)



Recommendation:

Invite Insurance Companies to participate in standards development, licensing & labeling design and definition, identity and interoperability for more affordable “IoT insurability”

7/21/2023

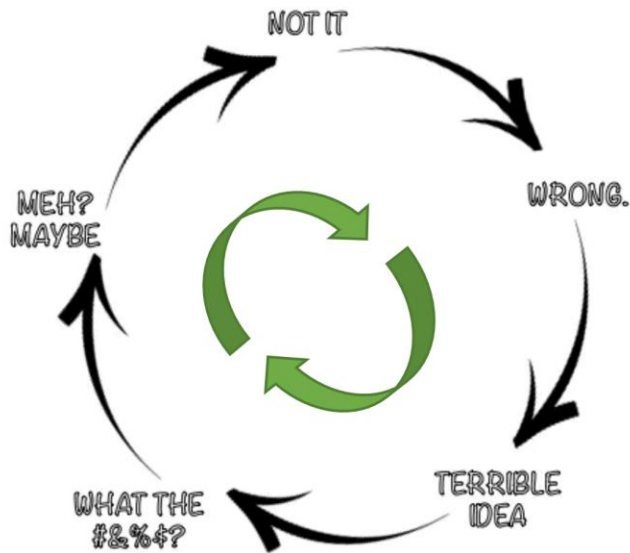
People Centered Internet, July 19, 2023



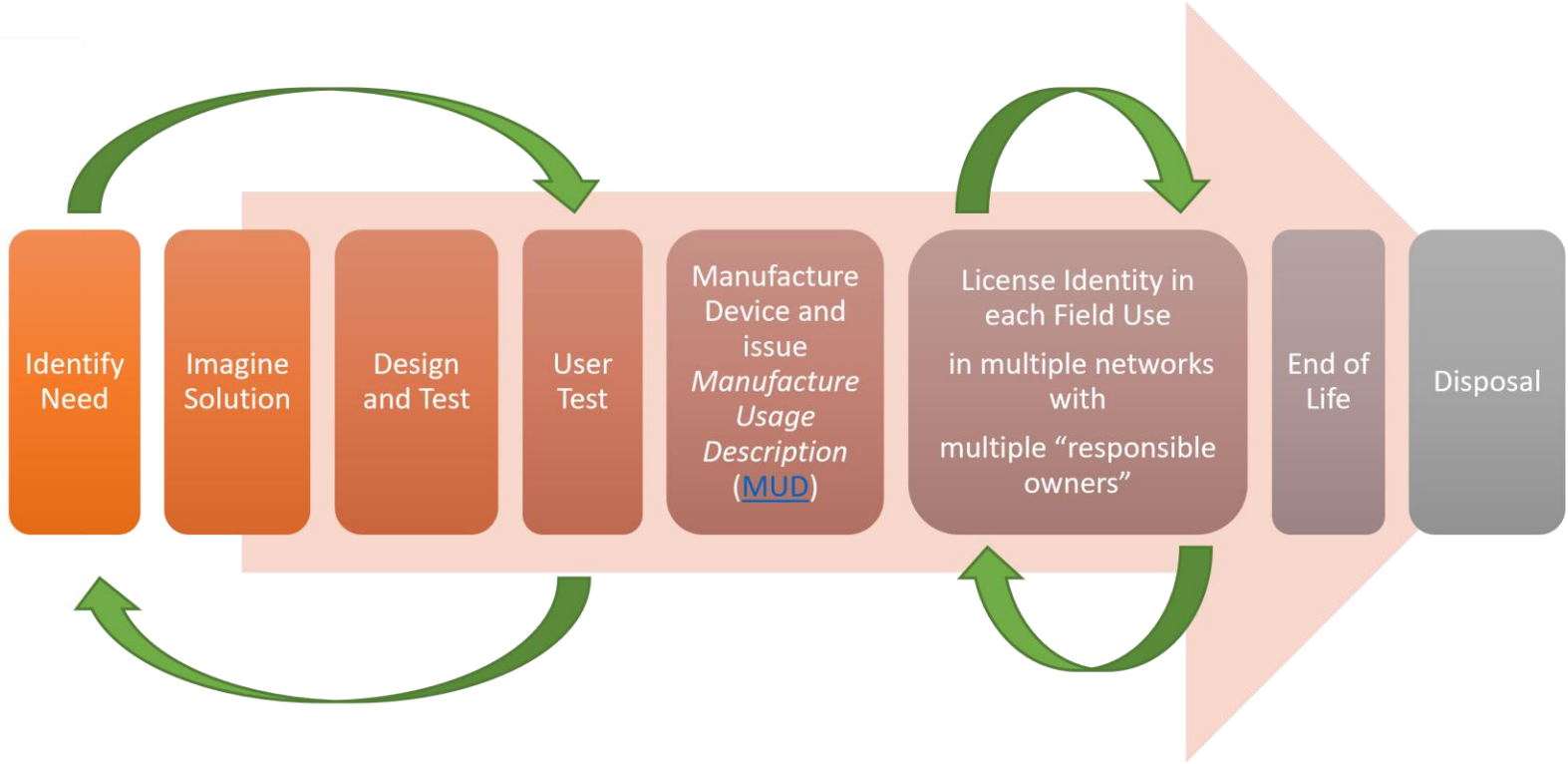
Identity evolves over the Lifecycle of an IoT Device



THE ITERATION CYCLE:



@andiefletch



Time ->

<https://medium.com/dashbored/the-iteration-cycle-best-or-worst-cycle-a7ab9f0319af>

Inter-operability for IoT

Massive Commercial WIN for NIST to drive
US Global Digital Leadership

Many new entrants, interoperability needed to increase functionality, and drive down costs



Just one example: Agriculture

- IoT can be adopted to the full range of farm types & sizes, products, climates, constraints
- California – IoT here has global use cases
- More than 400 types of crops
- Full range of terrain, climate zones, etc.
- Water is a major issue around world

R. Tse

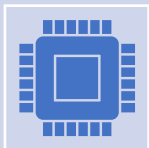
3 Barriers to Global IoT Adoption



Security and Privacy – no assurance of Responsibility by Maker



Specific Devices have no unique identity trackable through its Lifecycle



Expensive custom devices inhibit widespread use and increasing functionality; *Lack of standards increase upfront and operating cost*

3 Recommendations for Global IoT Adoption: L L I I

Label License

Responsible Tech Checklist & LABEL for each uniquely identified IoT LICENSE'd device

ID

Unique IDENTITY for each specific Device through its Lifecycle - via timestamp

INTEROP

INTEROPERABILITY & Standards For Internet Speed and Scale
Internet's Interop example ([link](#))

Can Internet of Things IoT be of the People, by the People, & for the People ?



YES!

with **LLIID**

1. **L**icensing IoT
2. **L**abeling IoT
3. **I**ntity for IoT – over lifecycle of device
4. **I**nter-operability – for massive WIN !

(if we put the guardrails in place for 1, 2, 3)

5. Bonus Recommendation: **D**igital Common Law ([link](#)) has been proposed at G7 Germany and G7 Japan Think7.org, UN Global Digital Compact, to be proposed G7 Italy G7 to evolve laws and regulations always obeying national law, where local communities can make their own decisions while citing precedents from elsewhere

Our Final Recommendation:

The People Centered
Internet Community
has the expertise and
willingness to deliver
on recommendations

We need to create a People Centered IoT that focuses the technology to be helpful, honest, and harmless.

It is likely in the next 20 years we will have trillions of Intelligent IoT achieving complex goals.

We need to ensure these goals are aligned with humanity's goals, the

UN SDGs by 2030 & thereafter.

D. Houhulin

Appendix

Page

| | |
|-------|---------------------|
| 15 | Mei Lin Fung bio |
| 16-20 | PCI Community Input |
| 21 | Label references |
| 22 | Identity references |

Mei Lin Fung Chair and cofounder with [Vint Cerf](#) of [People Centered Internet](#) is an early pioneer of customer relationship management (CRM) and is Alumni of Shell, Intel & Oracle. She holds a master's in Finance from MIT. She was socio-technical lead for US DoD's Federal Health Futures and founding chair of IEEE Technical Committee on Sustainability for the Society for Social Implications of Technology. Together with [Douglas Engelbart](#) she organized 2008 the [Program for the Future](#) and with Vint Cerf she organized 2014 the [40th Anniversary of the Internet](#). She is a Fellow of the Hasso Plattner Institute, recognized for her work on Digital policy including Clean-IT and energy-efficient computing. She hold the [Keynote on Decade of Digital Transformation](#) at the World Bank IFC Global SME Financing Forum and convenes the Digital Cooperation and Diplomacy network, a monthly forum for UNDP and ITU to interact with public and private sector thought leaders. She chairs Digital Week @UN Science Summit and champions in the ITU, Regional Digital Cross Sector regulation. Mei Lin was Vice Chair for Internet Inclusion for the IEEE Internet Initiative and served as one of the two co-chairs of the Expert Roundtable for Asia-Pacific, Europe, Africa and the Middle-East which developed recommendations for the 2023 UN Commission on the Status of Women report on Innovation and Technological change, and Education in the digital age. She is organizing the 50th Anniversary of the Internet with ITU and IEEE. Mei Lin was born in **Singapore**, studied, worked and married in **Australia** and lived in Silicon Valley, **California** for 4 decades. She led the 2022 policy input to the [German Think7 process with 11 policies](#) out of 70 policies in the final Communiqué contributed to by the People Centered Internet Community. She is the lead author for the Japan 2022 Think7 policy brief [People-Centered Science and Digital Transformation: A Practical Proposal for the G7 and G20](#).

People Centered Internet Community Input 1/5

| | | |
|------------------|-----------------------------|--|
| Vint Cerf | vgcerf@gmail.com | Desirable Properties of an IoT Ecosystem https://drive.google.com/file/d/1b_gu1evm5ZHGGmuezOrKSsgoZZ-9kQ/view?usp= |
| Albert Boulanger | aboulanger@worldteamnow.org | <p>The IOT needs the intelligent enablement for devices to self-tag. Tags in traditional SCADA are manually assigned. Devices need to be aware by a discovery mechanism or imprinted with their role/position in the system they are embedded in, like I am the outside air temp sensor of the 10th floor NW corner air handler to generate its smart tag. There is a lot of related work and good architecture, like IEEE 1451 smart transducer standards https://en.wikipedia.org/wiki/IEEE_1451, including Transducer electronic data sheets (TEDS), SensorML (OGC) https://en.wikipedia.org/wiki/SensorML, Semantic Sensor WEB (OGC) https://en.wikipedia.org/wiki/Semantic_Sensor_Web and Sensor Grid https://en.wikipedia.org/wiki/Sensor_grid and more. Here is a 2005(!) as-is/to-be diagram from How Martingale stochastic control navigates computer-aided lean energy management Oil & Gas Journal Volume: 103 Issue: 35 September 19, 2005, Roger Anderson Albert Boulanger.</p> <p>I believe full realization of what could be done with this as still lacking.</p> <p>http://tiger.aboulanger.com/web/lean/oqi/oqi-9-19-05_files/cap_z050919ogjxan03.gif</p> |
| Deborah Kobza | dkobza@certifiedisao.org | <p>The security of connected products and systems (IoT) continues to be of critical concern for consumers, and public-private organizations on a national, and global scale, with exploited vulnerabilities, malware, denial-of-service, and other attack vectors taking control and subverting the operations of IoT connected systems - impacting public health and safety, and national, global security. 'Security-by-Design' and "Security-by-Default" including implementation of "Zero-Trust" protocols and technology, and continued information sharing of 'actionable' security intelligence and coordinated response within and across public-private critical infrastructure sectors are paramount to ensure and sustain IoT security resilience.</p> |
| Alexa Raad | araad@alexaraad.com | <p>adding to the challenges is the fact that IoT devices introduce new security and privacy challenges because of limited processing capability, lack of high interconnectivity and high interactivity with the physical world and interaction with cloud services. In addition because of lack of data privacy regulation there is little privacy and transparency. In other words IoT devices are passively collecting personal information and the average consumer has little transparency and limited means to understand the data that is being collected and then shared.</p> <p>Another issue is the skills gap. Although cybersecurity industry has been plagued with this for a while now, it is worse when considering IoT and cybersecurity and the problem will only get worse as these devices proliferate,</p> |
| Dan Esbensen | misterdan@gmail.com | <p>Given that at some point, either Quantum computers or advanced Artificial Intelligence will be able to break all of the public key encryption that IOT devices use, how serious of a problem is this?</p> |

People Centered Internet Community Input 2/5

Linton Wells

linwells@gmail.com

NIST has a major project underway on: "Cyber-Physical Systems/Internet of Things for Smart Cities"
<<https://www.nist.gov/programs-projects/cyber-physical-systemsinternet-things-smart-cities>>

Two key concepts shape this program.

The first is the need to consolidate the vast amount of insights developed and collected from the previous smart city program and formalize them into a portfolio of publications and guidelines.

The second concept is the need to identify opportunities to support standards development processes for smart cities and communities technologies.

It has 3 sub-programs related to this:

The CPS/IoT Program: develops and demonstrates new measurement science and promotes the emergence of consensus standards and protocols for advanced cyber-physical systems and IoT that are scalable, effective, measurable, interoperable, trustworthy, and assured.

Testbed: The IoT/CPS Program is addressing this need through the development of a cross-sector CPS/IoT testbed based on co-simulation and consensus-based design principles for modular, composable testbeds that are interoperable with facilities across the nation and around the world for varying scale and readily reconfigurable for work across the nation and around the world for varying scale and readily reconfigurable for work across domains and applications.

Foundations: This project addresses these limitations through the development and application of a CPS Framework (applicable to CPS and IoT) to serve as a foundation for shared development, information exchange, and new formal methods applicable across domains.

In addition, NIST has a Special Publication on "Cyber-Physical Systems and the IOT." SP 1900-202
<<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1900-202.pdf>> So they've done, and are doing, a lot of work on this.

My biggest concern would be: how is NIST's excellent work being adopted in the field, especially abroad? My perception is that the economic incentives related to IOT are (1) functionality, and (2) speed to market. Security doesn't place very high in what's being bought. I'd be glad to be corrected on this, but it seems as though we are building smart cities around the world on a foundation of sand based on IoT insecurity. So my question to them is: (1) How is this changing? and (2) What can we do to see the standards adopted more thoroughly and quickly?

Comments welcome. I also agree with Mister Dan's point about the pending threat from quantum computing and advanced AI, but I just think we have an even more dangerous current threat.

People Centered Internet Community Input 3/5

| | | |
|-------------------|----------------------------------|--|
| Chris Swan | chris@swanz.net | <p>Hopefully you're already aware of the manufacturer usage description (MUD) draft RFC, but just making sure (as it's a good fit for your labels interest). https://datatracker.ietf.org/doc/html/rfc8520 Eliot Lear at Cisco has a couple of posts explaining the background and how it can help with some of the issues that have cropped up with IoT: https://ofcourseimright.com/?p=1859 https://ofcourseimright.com/?tag=mud</p> |
| Jennifer Hegelson | NIST | <p>there is a nascent piece of work - to automate the labeling - under community resilience - NLP - being user tested at U of MD - ask for a demo. Researchers spending a long time on labeling - so learn from the human, scan frequency of terms - makes a suggestion an highlights a short paragraph the "theme" then human collects - an approach to taxonomy and label to do intensive content analysis to understand pieces - qualitative content analysis - under AI umbrella - idea of article on Digital Observatory - analysis of text, understand frequency, bridge what human gets out of it, updates logic</p> |
| Robert Tse | rtse2@mac.com | <p>The rapid development of agriculture technology aka precision agriculture devices and its critical role for 21st century farm suffers from the lack of interoperability as one of two major constraints. The other is broadband. NIST could contribute to resolution of this challenge by helping develop interoperable standards that will enhance the use of the thousands of new agriculture technology devices on farm, encourage continued innovation by new entrants, help farmers obtain the maximum benefit of IoT devices that are integrated seamlessly into farm operations. This will also help farmers integrate and normalize climate adoption technology into farm operations. https://youtu.be/m8oTtS8duDc Here is the use case for interoperability between farm machines. I would expand this further to include all on farm IoT devices."</p> |
| Marc Goldberg | marc.goldburg@stanfordalumni.org | <p>Security principles for the devices themselves, for the protocols they use to communicate with other devices/services including cloud platforms (Google Home/Nest, Apple Homekit, Amazon Alexa), and for the cloud platforms themselves. Safety of life considerations, e.g., hacks of alarm, energy (e.g., residential solar power systems), medical, HVAC and even EV Things Privacy considerations, e.g., unauthorized/undesired access to in-workplace or in-home video, audio and motion sensor Things and their cloud platforms. Also, whether there are safeguards to prevent correlation of an individual's IoT data across multiple platforms/vendors to create a more comprehensive record of their activities than is available from any single platform. The last two might be considered subcategories of "security."</p> |
| Paul Werbos | pwerbos@gmail.com | <p>In the UN conference this morning, they emphasized civilian markets. As I recall, the official US speaker urged us to pay attention to these NIST actions, but for the civilian side. On the CIVILIAN side... I would still emphasize the need to develop and deploy more powerful, advanced technologies to harden cybersecurity for MANY areas (like what the earlier IEEE EPC motion called for). For the hardware side... we need to develop "quantum bromium", the massive improvement which can be enabled by true Quantum Annealing (true Quantum AGI, as we have discussed before. Most of the knowledgeable speakers this morning (like the main speaker from IA/CAS) gave strong emphasis to the cybersecurity urgencies both in civilian and military sectors. They all called for better open source detection of objects in the sky, which is dual use civilian (especially NASA) and military. Work plans for use of QAGI in seeing the sky, for shared open transparent use, would be our very best hope, in my view. Science France says they want new partnerships with US in many areas, such as quantum, but we will see how far they REALLY go this evening at their open house. I plan to be very quiet and listen a lot. Science France says they want new partnerships with US in many areas, such as quantum, but we will see how far they REALLY go this evening at their open house. I plan to be very quiet and listen a lot.</p> |

People Centered Internet Community Input 4/5

| | |
|--|--|
| <p>Doug Hohulin</p> <p>doug.hohulin@gmail.com</p> | <p>I agree the focus needs to be on security and privacy My one statement would be We need to create a People Centered IoT that focuses the technology to be helpful, honest, and harmless. It is likely in the next 20 years we will have trillions of Intelligent IoT achieving complex goals. We need to ensure these goals are aligned with humanities goals (UN SDG). I fed the this email chain and my statement into Claude and ask for a statement and 10 actions points, here is the response Claude We need to create a People Centered IoT that focuses the technology to be helpful, honest, and harmless. As we approach a future with trillions of Intelligent IoT devices collaborating autonomously to achieve complex goals, we must proactively align these technological capabilities with ethical priorities that serve humanity's wellbeing. Through establishing frameworks for accountable AI, prioritizing security/privacy by design, incentivizing openness and interoperability, and strengthening public-private partnerships, we can steer IoT innovation toward supporting human dignity, sustainability, justice and empowerment for all. With intention and vigilance, the promise of this technological revolution can be harnessed to uplift humanity and accelerate progress on the UN Sustainable Development Goals. Here are 10 action points I would suggest for NIST regarding People Centered IoT: Prioritize security and privacy from the ground up in IoT device and system design. Build trust through transparency. Develop standards and best practices for data minimization - only collect what is needed. Give users control over their data. Create frameworks for accountable AI in IoT - ensure fairness, explainability, and human oversight. Incentivize interoperability and open standards. Break down data and technology silos. Establish methodologies to assess societal impacts early and often. Consult diverse voices. Champion user-centric design, accessibility, and inclusion. Enable technology self-determination. Promote sustainability - ensure IoT lifespan, repair, recycling, and environmental impacts are considered. Build capacity for cybersecurity workforce, digital literacy, and community participation. Partner with other agencies, industry, and civil society to realize shared goals. Lead by example. Create roadmaps for positive technological futures - guide innovation toward serving social good. I gave presentations on the IoT and 6G/WiFi. Here is additional material that may be of use 6G White Paper on Edge Intelligence - 6G Flagship we are constantly assisting at an evolution from the "Internet of Things" to the "Internet of Intelligent Things". There is a need for an "Intelligent Internet of Intelligent Things" to make such internet more reliable, more efficient, more resilient, and more secure. This is exactly the area where 6G communication with edge-driven artificial intelligence can play a fundamental role."</p> |
| <p>David Bray, PhD</p> <p>david.a.bray@gmail.com</p> | <p>Building on Paul's comments - in 2019 I was invited to give a keynote to the United Nations on UN Charter Day re: what the future might have in store re: AI, IoT, and other advances in technologies. https://www.un.org/en/academic-impact/unai-charter-day-lecture-technology-data-and-future-un From that 2019 talk the same thing I would suggest to NIST is the crucial question: Can open societies, to include democratic nations, benefit from IOT to inform more effective local and national decision-making while simultaneously reinforcing and preserving personal privacy? ... because if we don't answer that question, autocracies will race ahead in using IOT for their social ends and/or open societies will erode privacy protections in order to benefit from IOT. We have to demonstrate better ways forward with IOT to provide benefits to communities will reinforcing individual freedoms include the right to be forgotten and choose when and where information about us is shared.</p> |
| <p>Brian Donohue</p> <p>briandonohuelaw@gmail.com</p> <p>7/25/2023</p> | <p>NIST needs to develop national standards for the healthcare industry for the most effective clinical use of the Social Determinants of Health People Centered Internet, July 19, 2023</p> |

People Centered Internet Community Input 5/5

| | | |
|---------------|----------------------------------|--|
| Robert Tse | rtse2@mac.com | <p>The rapid development of agriculture technology aka precision agriculture devices and its critical role for 21st century farm suffers from the lack of interoperability as one of two major constraints. The other is broadband. NIST could contribute to resolution of this challenge by helping develop interoperable standards that will enhance the use of the thousands of new agriculture technology devices on farm, encourage continued innovation by new entrants, help farmers obtain the maximum benefit of IoT devices that are integrated seamlessly into farm operations. This will also help farmers integrate and normalize climate adoption technology into farm operations. https://youtu.be/m8oTtS8duDc Here is the use case for interoperability between farm machines. I would expand this further to include all on farm IoT devices."</p> |
| Marc Goldberg | marc.goldburg@stanfordalumni.org | <p>Security principles for the devices themselves, for the protocols they use to communicate with other devices/services including cloud platforms (Google Home/Nest, Apple Homekit, Amazon Alexa), and for the cloud platforms themselves.</p> <p>Safety of life considerations, e.g., hacks of alarm, energy (e.g., residential solar power systems), medical, HVAC and even EV Things</p> <p>Privacy considerations, e.g., unauthorized/undesired access to in-workplace or in-home video, audio and motion sensor Things and their cloud platforms. Also, whether there are safeguards to prevent correlation of an individual's IoT data across multiple platforms/vendors to create a more comprehensive record of their activities than is available from any single platform.</p> <p>The last two might be considered subcategories of "security."</p> |
| Paul Werbos | pwerbos@gmail.com | <p>In the UN conference this morning, they emphasized civilian markets. As I recall, the official US speaker urged us to pay attention to these NIST actions, but for the civilian side.</p> <p>On the CIVILIAN side... I would still emphasize the need to develop and deploy more powerful, advanced technologies to harden cybersecurity for MANY areas (like what the earlier IEEE EPC motion called for). For the hardware side... we need to develop "quantum bromium", the massive improvement which can be enabled by true Quantum Annealing (true Quantum AGI, as we have discussed before.</p> <p>Most of the knowledgeable speakers this morning (like the main speaker from IA/CAS) gave strong emphasis to the cybersecurity urgencies both in civilian and military sectors. They all called for better open source detection of objects in the sky, which is dual use civilian (especially NASA) and military.</p> <p>Work plans for use of QAGI in seeing the sky, for shared open transparent use, would be our very best hope, in my view.</p> <p>Science France says they want new partnerships with US in many areas, such as quantum, but we will see how far they REALLY go this evening at their open house. I plan to be very quiet and listen a lot.</p> <p>Science France says they want new partnerships with US in many areas, such as quantum, but we will see how far they REALLY go this evening at their open house. I plan to be very quiet and listen a lot.</p> |

References on Labels

- Brewers, Paula. [“The History of Labels.”](#) *Navitor*. ImpressionsBlog. 4 Sept. 2013.
- Cavoukian, Ann. [Privacy by Design: The 7 Foundational Principles](#). Toronto, ON: Information and Privacy - Commissioner of Ontario, 2011.
- [“EstándaresIberoamericanos”](#) (“Standards for Personal Data Protection for Ibero-American States”). Red Iberoamericana de Protección de Datos, Documentos, EstándaresIberoamericanos (website).
- European Parliament and the Council of the European Union. [Regulation \(EU\) 2016/679 of the European Parliament and of the Council of 27 April 2016](#). *Official Journal of the European Union*. 4 May 2016.
- Food Insight. [“The Nutrition Facts Label: Its History, Purpose and Updates.”](#) Food Insight (website). 9 Mar. 2020.
- Janssen, Wallace F. [“The Story of the Laws Behind the Labels.”](#) FDA Consumer. June 1981.
- Tiberio, Guy. [Vehicle Information Labels: The Stickers You Need to Know!](#) (slide presentation).

References on IoT identity

Manufacturer usage description (MUD) draft RFC:
<https://datatracker.ietf.org/doc/html/rfc8520>

Eliot Lear at Cisco has a couple of posts explaining the background and how it can help with some of the issues that have cropped up with IoT:

<https://ofcourseimright.com/?p=1859>

<https://ofcourseimright.com/?tag=mud>