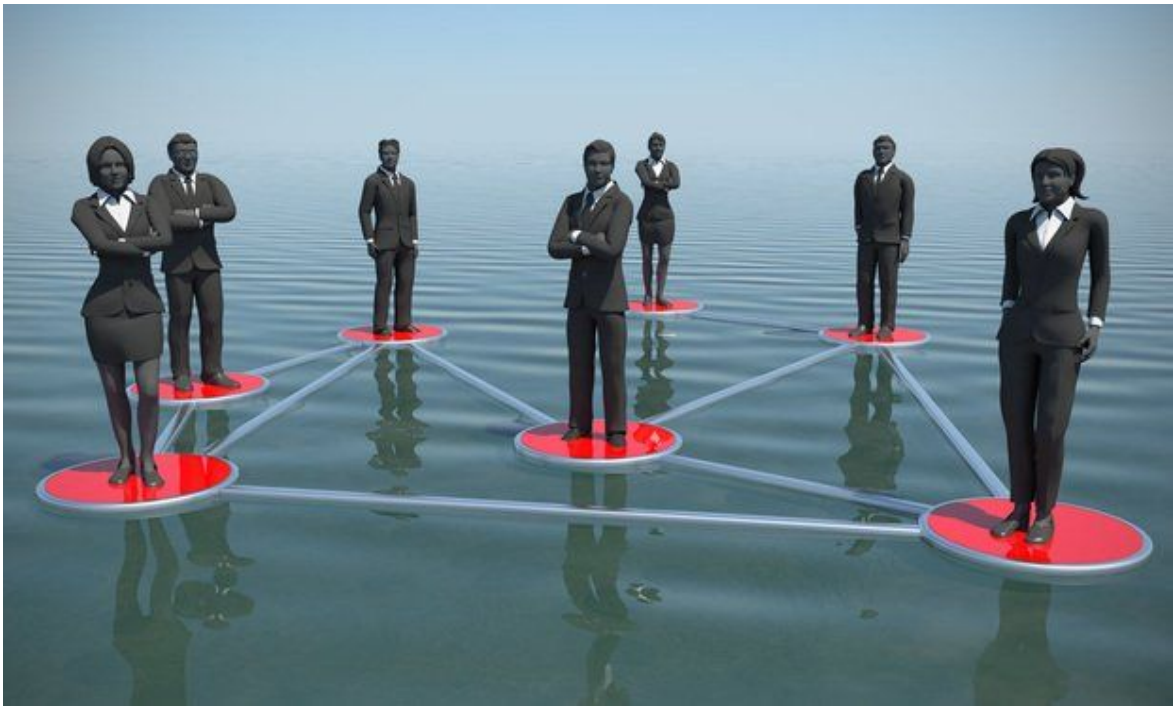


Internet Of Bodies: Creepy New Platform For Data Discovery

Technocrats are moving from collecting external data about you to collecting data from inside you, underscoring the point that there is no level of detail that satisfies a Technocrat. From the macrocosm to the microcosm, every piece of data must be collected. TN Editor

In the Era of the Internet of Things, we've become (at least somewhat) comfortable with our refrigerators knowing more about us than we know about ourselves and our Apple watches transmitting our every movement. The Internet of Things has even made it into the courtroom in cases such as the hot tub saga of Amazon Echo's Alexa in *State v. Bates* and an unfortunate wife's Fitbit in *State v. Dabate*.

But the Internet of Bodies?

Yes, that's right. It's gone beyond the mere snooping of a smart TV. Data discovery has entered a new realm, and our bodies are the platform.

A January 5 program at the Annual Meeting of the Association of American Law Schools (AALS) in New Orleans entitled, *The Internet of Bodies: Cyborgs and the Law*, discussed the legal, regulatory, and societal impact of this new living and breathing platform for data discovery.

Internet of Bodies?

First things first: What is the Internet of Bodies?

“The Internet of Bodies refers to the legal and policy implications of using the human body as a technology platform,” said Northeastern University law professor Andrea Matwyshyn, who works also as co-director of Northeastern’s Center for Law, Innovation, and Creativity (CLIC).

“In brief, the Internet of Things (IoT) is moving onto and inside the human body, becoming the Internet of Bodies (IoB),” Matwyshyn added.

Joining Matwyshyn on the AALS panel were moderator Christina Mulligan, professor of law and vice dean at Brooklyn Law School; Nancy Kim, professor at California Western School of Law; and Robert Heverly, associate professor at Albany Law School. Elizabeth Rowe, professor of law and director of the intellectual property law program at the University of Florida Levin College of Law, assisted in the development of the program.

The Internet of Bodies is not merely a theoretical discussion of what might happen in the future. It’s happening already.

Former U.S. Vice President Dick Cheney revealed in 2013 that his physicians ordered the wireless capabilities of his heart implant disabled out of concern for potential assassin hackers, and in 2017, the U.S. Food and Drug Administration recalled almost half a million pacemakers over security issues requiring a firmware update.

It’s not just former vice presidents and heart patients becoming part of the Internet of Bodies. Northeastern’s Matwyshyn notes that so-called “smart pills” with sensors can report back health data from your

stomach to smartphones, and a self-tuning brain implant is being tested to treat Alzheimer's and Parkinson's.

So, what's not to like?

Better with Bacon?

"We are attaching everything to the Internet whether we need to or not," Matwyshyn said, calling it the "Better with Bacon" problem, noting that—as bacon has become a popular condiment in restaurants—chefs are putting it on everything from drinks to cupcakes.

"It's great if you love bacon, but not if you're a vegetarian or if you just don't like bacon. It's not a bonus," Matwyshyn added.

Matwyshyn's bacon analogy raises interesting questions: Do we really need to connect everything to the Internet? Do the data privacy and data protection risks outweigh the benefits?

The Northeastern Law professor divides these IoB devices into three generations: 1) "body external" devices, such as Fitbits and Apple watches, 2) "body internal" devices, including Internet-connected pacemakers, cochlear implants, and digital pills, and 3) "body embedded" devices, hardwired technology where the human brain and external devices meld, where a human body has a real time connection to a remote machine with live updates.

Chip Party for Chipped Employees

A Wisconsin company, Three Square Market, made headlines in 2017—including an appearance on The Today Show—when the company microchipped its employees, not unlike what veterinarians do with the family pet. Not surprisingly, the company touted the benefits of implanting microchips under the skin of employees, including being able to wave one's hand at a door instead of having to carry a badge or use a password.

CNBC reported that 50 of Three Square Market's 80 employees volunteered to have the microchips implanted under their skin, and they

even had a so-called chip party, where the radio frequency identification (RFID) microchips—about the size of a grain of rice—were injected into the employees.

However, where the employees really “volunteers”?

California Western’s Kim noted that consent is an important issue for the Internet of Bodies and that it’s an especially challenging issue when the IoB involves employees, who depend on their employers for a paycheck.

In addition, she thinks that having the chip party was a really bad idea.

“I think it impedes the consent condition of voluntariness. They should not have had a chip party on their premises. It shouldn’t be onsite where everyone knows who got chipped and who didn’t. It’s coercive in its nature even if it’s not a mandatory requirement,” Kim said.

Read full story here…

Ford To Deploy 5G Vehicle-To-Everything Tech By 2022

Ford Motor Company will be the first to use 5G to enable ubiquitous communication between autos, traffic signals, cell phones. This also gives a clue as to when 5G will be fully rolled out to the nation. TN Editor

Don Butler, executive director of the Ford Connected Vehicle Platform and Product, announced in a Medium post on Monday that Ford has committed to deploy cellular vehicle-to-everything (C-V2X) technology in all new U.S. vehicle models starting in 2022.

The C-V2X tech will allow equipped vehicles to "talk" to and "listen" to each other, as well as directly connect with traffic management infrastructure (such as traffic lights). Pedestrians can also use their mobile phones to convey their locations to vehicles, making roads safer for walkers and cyclists.

"Driver-assist technologies today and autonomous vehicles of the future utilize on-board sensors much in the way people use their eyes to navigate complex environments," Butler wrote. "C-V2X could complement these systems in ways similar to how our sense of hearing complements our vision to improve our ability to operate in a complex world."

5G isn't just changing how society will utilize the internet — it's also transforming how vehicles can connect with their surrounding environment. The C-V2X platform will run on 5G and complement any existing LiDAR, radar and camera sensors for a "comprehensive view" of the road and infrastructure. According to Butler, the timing of this effort by Ford is "perfect," considering the cellular industry's push toward building 5G networks. However, the road ahead is still long — Ford acknowledges it must work with fellow automakers and government organizations in order to "create such a technology-neutral environment."

Successful deployment would significantly impact pedestrian safety and traffic accidents. As cities invest in Vision Zero efforts, there may be advantages to working with automakers such as Ford to enhance these technologies and ensure that they fit into the city's overall safety goals.

Read full story here…

Should A Self-Driving Car Kill The Baby Or The Grandma?

Different cultures give different answers, and the there is obviously no rigid commonality between nations. When AI programs are created, however, they must start with a moral judgement as to how their programs will behave. TN Editor

The infamous "trolley problem" was put to millions of people in a global study, revealing how much ethics diverge across cultures.

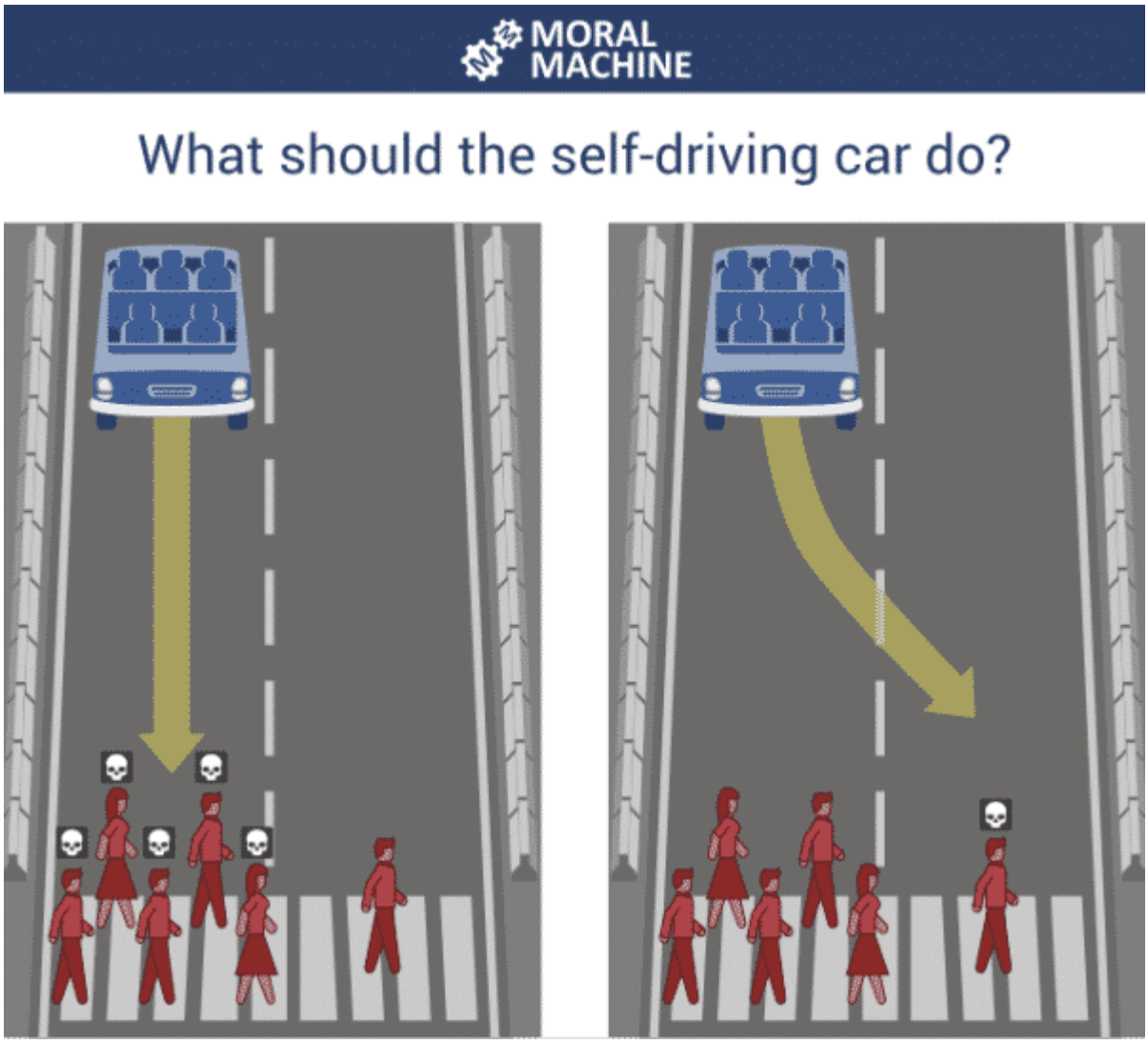
In 2014 researchers at the MIT Media Lab designed an experiment called Moral Machine. The idea was to create a game-like platform that would crowdsource people's decisions on how self-driving cars should prioritize lives in different variations of the "trolley problem." In the process, the data generated would provide insight into the collective ethical priorities of different cultures.

The researchers never predicted the experiment's viral reception. Four years after the platform went live, millions of people in 233 countries and territories have logged 40 million decisions, making it one of the largest studies ever done on global moral preferences.

A new paper published in *Nature* presents the analysis of that data and reveals how much cross-cultural ethics diverge on the basis of culture, economics, and geographic location.

The classic trolley problem goes like this: You see a runaway trolley speeding down the tracks, about to hit and kill five people. You have access to a lever that could switch the trolley to a different track, where a different person would meet an untimely demise. Should you pull the lever and end one life to spare five?

The Moral Machine took that idea to test nine different comparisons shown to polarize people: should a self-driving car prioritize humans over pets, passengers over pedestrians, more lives over fewer, women over men, young over old, fit over sickly, higher social status over lower, law-abiders over law-benders? And finally, should the car swerve (take action) or stay on course (inaction)?



Rather than pose one-to-one comparisons, however, the experiment presented participants with various combinations, such as whether a self-driving car should continue straight ahead to kill three elderly pedestrians or swerve into a barricade to kill three youthful passengers.

The researchers found that countries' preferences differ widely, but they also correlate highly with culture and economics. For example, participants from collectivist cultures like China and Japan are less likely to spare the young over the old—perhaps, the researchers hypothesized, because of a greater emphasis on respecting the elderly.

Similarly, participants from poorer countries with weaker institutions are more tolerant of jaywalkers versus pedestrians who cross legally. And participants from countries with a high level of economic inequality show greater gaps between the treatment of individuals with high and low social status.

And, in what boils down to the essential question of the trolley problem, the researchers found that the sheer number of people in harm's way wasn't always the dominant factor in choosing which group should be spared. The results showed that participants from individualistic cultures, like the UK and US, placed a stronger emphasis on sparing more lives given all the other choices—perhaps, in the authors' views, because of the greater emphasis on the value of each individual.

Read full story here…

China Seeks Global Control Over Internet Of Things For

Spying, Business

As a Technocracy, China is only doing what is natural to them: dominating the world of data collection, surveillance and control. The Western world has completely missed China's nefarious intentions as it has embedded Chinese technology as all levels of society. TN Editor

China is aggressively seeking to dominate the Internet of Things and plans to use access to billions of networked electronic devices for intelligence-gathering, sabotage, and business purposes, according to a forthcoming congressional report.

China for nearly a decade has been investing heavily in the emerging technology on the Internet of Things (IoT) and has made outpacing similar U.S. efforts one of the ruling Communist Party of China's highest strategic goals.

"China's unique approach to the development of IoT and its enabling infrastructure poses significant challenges for U.S. economic and national security interests," says a report by the U.S.-China Economic and Security Review Commission due out Thursday.

"The highest echelons of the Chinese regime view IoT development and deployment as critical matters of China's economic competitiveness and national security."

A major concern outlined in the report is China's efforts to uncover vulnerabilities in IoT systems that can be used by Beijing for strategic objectives in both peacetime and war, the report said.

"Aside from industrial control systems, unauthorized access to health care devices could kill patients and exploitation of smart car vulnerabilities could kill drivers and pedestrians alike, among other examples of possible misuse of data and devices that could have dire consequences," the report warns.

"The future destructive potential of unauthorized access to IoT devices appears potentially limitless."

The IoT is an ill-defined term for a global information and communication infrastructure. It is made up of linked devices ranging from biomedical devices for monitoring patients to self-driving cars to critical infrastructure.

The universe of IoT devices includes billions of electronic systems such as, video cameras, smart phones and smart watches, and industrial control systems used in electric grids.

Chinese IoT objectives include building "smart cities" that monitor public utilities, flows of people and traffic, underground pipelines, and air and water quality, the report said.

Other Chinese IoT plans include advanced remote industrial controls; medical IoTs; smart homes equipped with remote controls for appliances and security systems; and smart cars linking vehicle sensors to drivers, roads, cloud services, and other electronic devices.

The IoT is expanding rapidly and will be further enhanced with emerging advanced information technologies, such 5G cellular technology.

Use of 5G networks will increase the ability of networked devices to interact through faster data transfer speeds.

China, according to the report, is working on major programs to find vulnerabilities in IoT technology ostensibly for cyber security.

However, the report suggests the research is cover for plans to conduct for cyber espionage, sabotage, and military cyber reconnaissance using the Internet of Things.

One example of an IoT cyber attack took place in 2016 when the malware known as the Mirai botnet infiltrated thousands of linked devices by scanning the Internet for video cameras—most made in China—and DVRs that were not protected and easily accessed by using default passwords such as "password."

Mirai "commandeered some one hundred thousand of these devices, and used them to carry out a distributed denial of service (DDoS) attack against DynDNS that shut down many popular websites," the report

said.

A second botnet called IoTroop targeted several brands of Chinese-made Internet Protocol cameras in late 2017.

A Chinese case discovered in 2016 by security researchers revealed that firmware update software made by the Shanghai ADUPS Technology Co. Ltd. was secretly siphoning off private data and sending it to China.

"ADUPS's firmware update software is currently in use on more than 700 million low-end mobile phones and IoT devices around the globe, including devices in the United States," the report said.

Chinese IoT researchers also are preparing to use cyber attacks against the "Internet of Underwater Things" that has applications for submarine warfare.

"The imperfect availability of enemy location information in underwater warfare offers a strategic advantage to any nation with advanced underwater sensor technology, and compromised IoT devices and sensor networks operating underwater at a variety of depths could nullify any such advantage," the report said.

China also is preparing to use the IoT for intelligence gathering and network reconnaissance—the first step in cyber war.

"Personnel from several of the PLA's signals intelligence units have published multiple articles on IoT security-related topics, suggesting that these units have likely already exploited device vulnerabilities for these ends," the report said.

The Chinese military's cyber and computer attack force has written journal articles discussing the use of "emissions from IoT devices as possible avenues for side-channel attacks and listing location tracking features and internet connections as other weak points for exploitation," the report said.

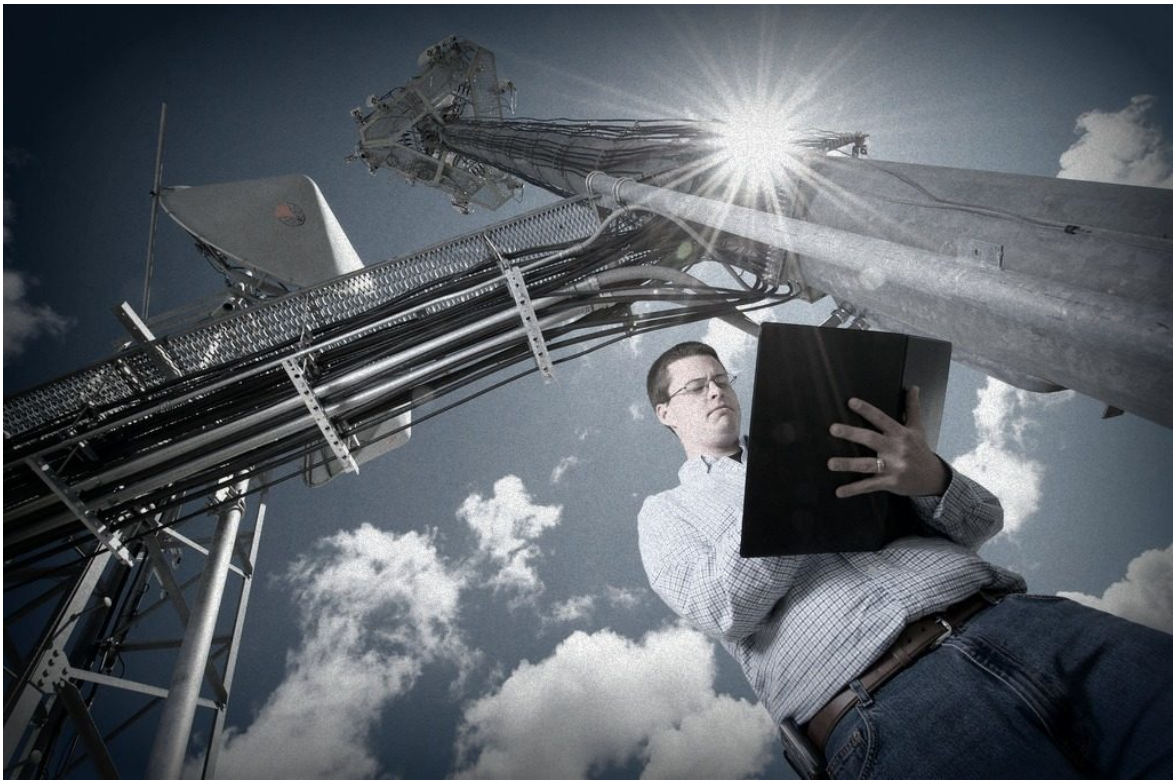
"The PLA's operational cyber warfare units have also previously shown direct interest in exploiting IoT security vulnerabilities for offensive information warfare," the report said, such as IoT data collection and

cellphone-transmitted viruses.

A PLA electronic warfare report said smart cars are very vulnerable to attack and unauthorized access through their internal car wireless sensor networks, car-mounted controller area network buses, car-mounted local area networking, car software applications, car-mounted onboard diagnostic systems, and smart tire-pressure monitoring systems.

China is also using the IoT to boost its mass internal security surveillance capabilities to control the Chinese people, the report said.

Read full story here…



Wireless Wars: When Censors

Control the Sensors

Technocracy is about using collected data to engineer and control all of society by a select few who believe they have the answers for mankind. This movement got traction in the 1930s but was rejected by American by the 1940s. Now, it's back and little has changed. TN Editor

The conveniences of the emerging explosion of artificial intelligence, machine-to-machine learning, and ubiquitous "5G" fifth-generation connectivity of the 4th industrial revolution may seem a far cry from the day that residential electrification made its way onto farms and into households.

But the problem with 4th industrial revolution, like all of the previous revolutions, is that in the name of progress, the implications regarding the Laws of Nature, the environment, and human health do not have a seat at the table. Yet.

Four Revolutions of Unacknowledged Harm

According to *Digital Pulse of Australia*, **"The first industrial revolution was about coal, water and steam,** bringing with it the steam engine and innovations that enabled the large scale manufacturing of goods and products.

The second industrial revolution came about with the invention of electricity and enabled mass production (think production lines). Dating from the late 1800s to early 1900s, from this phase emerged the internal combustion engine, and thus the automobile. The period was marked with an increased use of steel and eventually petroleum, and the harnessing of electric current. It allowed much of the progress of the first industrial revolution to move beyond cities and achieve scale across countries and continents.

The third industrial revolution was all about computers. From the 1950s onwards, computers and digital systems enabled new ways of processing and sharing information. Transistors, microprocessors, robotics and automation – not to mention the internet and mass

communications – would eventually allow for the ultimate in scale: globalisation.

Which brings us to the fourth industrial revolution, also referred to as Industry 4.0. According to the World Economic Forum which coined the phrase, the 4th industrial revolution is one of "cyber-physical systems" – that is, the merging of the capabilities of both human and machine.[1] This is the era of artificial intelligence, genome editing, biometrics, renewable energy, 3D printing, autonomous vehicles and the Internet of Things.[1]

As the World Economic Forum pointed out, however, "while the Fourth Industrial Revolution may look and feel like an exogenous force with the power of a tsunami, […] in reality, it is a reflection of our desires and choices." Navigated wisely, the Fourth, will bring us smart cities that reduce poverty and enhance standards of living, sustainable energy sources, environmental protection, more inclusive government process, social cohesiveness and collaboration, and make us healthier.

In 2017, the World Economic Forum opened a Center for the Fourth Industrial Revolution in San Francisco. "Artificial intelligence, national digital policies, cross-border data flows, drones, autonomous vehicles and environmental technology will all be discussed at the center, alongside any new innovations that come out of Silicon Valley or another tech hub." "The 4th revolution is reshaping industries, challenging existing regulatory frameworks, and redefining what it means to be a human," said Murat Sönmez, Member of the Managing Board and Head of the Center.

The Fourth Failure to Apply Precaution; Manipulating the Masses

The 4th industrial revolution is being widely promoted as a strategy to address the pollution that was created using the fossil fuel model of progress. Environmental and health advocates are promoting research focused on the negative impact of air pollution particulate matter on children's health.

These studies are being used to promote smart cities with wireless

sensors that measure air pollution in real-time, [7] [8] while ignoring the fact that the system of wireless sensors and supporting antennas is creating air pollution in the form of electrosmog. We are in fact introducing a second form of air pollution with known health and environmental consequences, in order to quantify the first form of air pollution.

Regarding the claims that artificial intelligence will reduce poverty, as an example, the USDA has employed the use of an algorithm in its crusade against SNAP (Supplemental Nutrition Assistance Program). *Truthdig*reported:

> *In February, Trump suggested that most recipients should receive half of those benefits not in money they can spend as they see fit but in the form of a box of shelf-stable packaged foods, which the administration said would reduce the overall cost of the program by $129 billion over the next 10 years. While neither the budget for SNAP nor the future of Trump's "box proposal" has yet to be determined, the U.S. Department of Agriculture has found other ways to punish both SNAP users and the stores at which they shop. On Monday, in collaboration with the nonprofit newsroom, New Food Economy, The Intercept published a report on a USDA algorithm, part of the department's ALERT system, that in 2017 disqualified over 1,600 retailers from accepting SNAP benefits.*

Alexa's and Siri's Big Fat Environmental Footprints

Claims regarding sustainability have ignored the burgeoning energy expenditure of monitoring the home air conditioner from a moving vehicle. As Katharine Schwab reported in *Fast Company* about the work of AI researcher Kate Crawford and data visualization specialist Vladan Joler.

To the user, asking Alexa a question is the epitome of ease. To the people who mined the minerals, built the speaker, and trained the AI, it's anything but. "Alexa, what time is it?"

> *"The mineral extraction, smelting, logistics, fiber optic cables, networking, AI training, energy, and e-waste . . . it's an almost*

impossible task, requiring a mind-boggling scale," Crawford says. "So we started by drawing multiple version on butcher's paper, and it took dozens of sheets."

From there, Joler and Crawford took a year to research every piece of the Echo's supply chain, uncover the hidden human labor that most of us don't think about when we query a voice assistant, and put it in historical, geological, and anthropological context.

It's not just the miners: It's also the humans operating the gigantic global shipping and manufacturing apparatus that brings each piece of the puzzle together, it's the click-workers who label and sort vast data sets on which to train AI, and it's you, the user, who is simultaneously acting as "a consumer, a resource, a worker, and a product," as Crawford and Joler write in the essay. Through this lens, Echo's complex processing becomes a story of human work and–more disturbingly–human exploitation. A child laborer in the mines of the Congo would need to work for 700,000 years without stopping to accumulate the kind of capital that Amazon CEO Jeff Bezos makes per day. "At every level contemporary technology is deeply rooted in and running on the exploitation of human bodies," Crawford and Joler write in the essay."

When the sensors are controlled by censors, we don't look at the range of health and environmental impacts of each rising rates of autism, neurological illnesses, electromagnetic sensitivity, neurological issues, DNA alterations, childhood cancers, and other illness associated with 5G and the 4th revolution. Thus far, the 4th revolution has resulted in the opposite of the World Bank's projections. We have more poverty, more concentrated wealth, and less citizen input as decision-makers cater to corporations and promises of economic expansion. And if we don't fix that problem right away, the sensors will only serve the censors.

Read full story here…

IoT Implementation in Renewable Energy Will Create New Cyber Attack Risks

The Internet of Things (IoT) will come alive with the implementation of 5G wireless communications, and everything 'Smart" will be connected to it. The Technocrats who came up with all this have little concern for security, so hacking will be a cake-walk for evil doers. TN Editor

Water, Wind and Solar energy (WWS) has the potential to replace diminishing and polluting fossil fuel, petroleum, coal and other traditional power sources in a way that can change the very course of our planet's future.

Sustainable energy is already driving positive changes throughout the world, even as we are still early in the process of scaling WWS and making naturally generated power available through more modern grids, in the developed and developing worlds.

The challenge of scale is being addressed by Internet of Things (IoT) and Industrial Internet of Things (IIoT) through instrumenting larger and

larger systems, including wind farms, water farms, hydroelectric dams, and more.

The IoT and IIoT, combined with the analytics and control systems connecting and managing sensors and other equipment will help harness clean power, but also manage that power through changes in demand by being able to store and ship power from a solar plant, for example, even through extended periods of cloudy weather.

The beauty of IoT and IIoT is in the mix: for example, with smart appliances in the home, individuals can understand and manage their own power usage to reduce their cost of energy and contribute to a more sustainable planet.

Those same consumers can allow their energy providers or suppliers of their appliances to remotely manage consumption of energy.

The energy providers can do this on a mass scale, with tens of hundreds of thousands of homes, and help entire communities conserve sustainable energy, thus improving the supply and demand cycles required for peak times, all while creating lasting improvements made possible when we make the switch in a systematic way from reliance on traditional to sustainable energy.

This works from the "top down" too, when utilities and municipalities work together to build new energy sources to serve businesses and consumers, leveraging new business models in the process (for example revenue sharing between the utility company and the government, with private-public partnerships emerging as part of not only "smart city" but "smart region" initiatives).

Coming from the ground up, or from larger, funded initiatives, this is all good – but are we missing something while imagining this new ideal world?

Security experts believe we are, and we're starting to see more and more publishing on the security threats associated with not just traditional nuclear, electric and hydroelectric plants, and the closely related energy and communications grid, but with sustainable energy

particularly when the day comes that we are applying as many sensors to that as we are applying to existing, aging infrastructure.

With sustainable energy systems instrumented, there are now tens of thousands of sensors and gateways at the edge of IoT/IIoT networks, where a huge amount of data is collected and analyzed, including electricity loads, wind energy volume based on blade resistance, solar panel temperatures and positions, and more. There is the potential to sense, measure, monitor and control any component that is electrified.

This data is also uploaded via networks to clouds for processing whatever is not being locally computed, and all this starts to add up to a growing attack surface which cyber criminals can leverage for hacking into systems (plants as well as homes and businesses) to gather information, to initiate denial of service attacks, to initiate a ransomware attack, and more.

Last year, David Vazquez Cheatham, at the UNM National Security Studies Program published a paper on "Security Readiness: Key Issues Within Civilian Critical Power Generation Infrastructure." In this paper, Cheatham noted:

"It has been known for decades that the US Power infrastructure contains key weaknesses in both physical and cyber security countermeasures. In addition, hardware design of primary control centers and critical components are in need of a major overhaul by design engineers building in features that will address the known cyber security weaknesses. In order to address physical security weaknesses across the US, a standard must be set with a system to both guide and hold accountable energy providers physical security of critical infrastructure. Despite calls for action from the scientific community, analysts and even congressmen there has been little headway. The need for upgrades has become critical in nature for our national defense due to threats from a range of attacks: physical, cyber, electromagnetic pulse, directed energy weapons and certain severe weather conditions can all wreak havoc."

Read full story here…

The Battle Between States And Cities To Control 5G

Thanks to carrier lobbying, twenty states have already passed legislation to strip their cities of the power to regulate 5G rollouts. Cities are fighting back with lawsuits to restore local control and ability to set fees and address health concerns. A Technocrat state Senator in Texas says, “We should keep government out of the way of technology and let technology get us all there.” TN Editor

Back in 2016, several major phone carriers approached the city of McAllen, Texas, about building state-of-the-art 5G wireless networks. With the promise of ultra-fast internet connection speeds and an array of potential commercial and public applications, city officials eagerly entered into discussions about amending local ordinances to accommodate the necessary infrastructure. Months later, they were close to reaching an agreement on establishing a large-scale pilot program.

It all started to unravel, though, when McAllen and other Texas cities heard about a proposal in the legislature setting statewide rules for 5G installation and prohibiting local governments from negotiating their own deals. McAllen City Attorney Kevin Pagan says the wireless providers initially assured him they weren't interested in asking for state legislative help. But then the bill started gaining traction. Company representatives stopped responding to Pagan's emails about the licensing agreement, and he says he hasn't heard from them since.

The legislation sailed through both chambers and was signed into law last spring. McAllen has joined other Texas cities as lead plaintiff in suing the state over the bill. "I'd like to say it was a fight, but when the score has already been determined in advance before the starting gun goes off, it's difficult to call it a fight," Pagan says. "Nothing that we suggested of any substance was [included] in S.B. 1004."

Across the country, telecom companies are beginning to lay the groundwork for 5G wireless networks. The buildout often pits states against cities, as in Texas. But a proposal that the Federal Communications Commission (FCC) is set to vote on Sept. 26 would not only upend future local agreements, but also preempt states. If approved, localities across the country would have drastically less authority over 5G infrastructure.

The arrival of 5G represents a major advancement in wireless technology. It's expected to provide speeds at least 10 times faster than the typical 4G connection that many places now have. Testing is underway in select cities, and the FCC will start auctioning licenses for 5G spectrum in November. The first 5G-compatible smartphones are expected to follow next year.

Some localities are already looking to use the technology in ways that go well beyond improving internet speeds. Kansas City, Mo., partnered with Cisco and Sprint on building a public Wi-Fi network covering part of the city's downtown. It supports pedestrian sensors and interactive kiosks along a streetcar line. Bob Bennett, Kansas City's chief innovation officer, envisions a litany of potential future applications once 5G is enabled. Air quality and temperature sensors detecting pollution, he

says, could play a role in determining where kids wait for buses. Others have hailed 5G as crucial for transmitting data to autonomous vehicles.

The key building blocks of 5G networks are small-cell antennas interwoven throughout city infrastructure, affixed to streetlights, utility poles or buildings. Providers typically describe them as the size of pizza boxes. But in actuality some of the antennas are much larger, while others are hardly noticeable at all. They generally need to physically connect to wireline fiber, so the first places expected to get 5G are densely populated urban areas with high consumer demand and existing fiber networks. One study conducted by the municipal advocacy group Next Century Cities, of jurisdictions considered to be leaders in technology, reported that 60 percent of communities with a wireline fiber connection to residences had small cells in place, while the same was true of only a third of those without existing fiber.

Unlike cellphone towers, small-cell nodes have limited range and poor ability to send signals through physical barriers. So telecoms may need to install hundreds of small cells to cover a relatively small area — an undertaking that becomes cost-prohibitive in less urbanized areas. For this reason, Blair Levin, a former FCC official who oversaw the National Broadband Plan, says 5G is likely to further widen the digital divide that has disadvantaged parts of rural America.

Supporters of the FCC proposal and state laws governing 5G frequently maintain that the laws will speed up construction, as well as potentially facilitate its use in currently unserved areas. In their pitches to Nebraska state lawmakers last year, lobbyists argued that a statewide rule would accelerate rural deployment. Citing comments provided by telecom providers, the FCC proposal similarly concluded that "resources consumed in serving one geographic area are likely to deplete the resources available for serving other areas."

But local officials contend that carriers won't bring their 5G networks to outlying areas absent market demand. "There is not a shred of evidence that suggests a penny saved in New York immediately gets invested in Montana," Levin says. McAllen's Pagan adds that his city offered companies a "healthy subsidy" to deploy internet service in unserved

areas, but they weren't interested.

What's certain is that the FCC wants to lower the cost of deployment. As of early this summer, 20 states had enacted legislation aimed at facilitating 5G small-cell deployment, according to the National Conference of State Legislatures. FCC Commissioner Brendan Carr has stated that the order wouldn't alter nearly any provisions of the 20 existing state laws. But any that do not satisfy the proposed federal rules would be preempted.

Read full story here…

AT&T Is Rolling Out 5G To Five Additional American Cities

At last count, the major telecom carriers are working on 5G rollout in

about 50 cities throughout America, including some second tier cities like Waco, Texas and Sacramento, California. The big surge of mass installation should be fully underway by mid-2019. This is not about cell phones, but rather factories, autonomous vehicles, ubiquitous collection of data from sensors, surveillance and Smart City technology. TN Editor

AT&T named the final five cities that will see the company's mobile 5G before the end of 2018: Houston; Jacksonville, FL; Louisville, KY; New Orleans; and San Antonio. The company also said it plans to launch in seven more cities — Las Vegas; Los Angeles; Nashville, TN; Orlando, FL; San Diego; San Francisco; and San Jose, CA — in early 2019.

The company also made the world's first wireless 5G data transfer over millimeter wave with standards-based production equipment on a mobile form factor device.

The five new cities join the seven that have already been announced as getting AT&T 5G in 2018: Atlanta; Charlotte, NC; Dallas; Indianapolis; Oklahoma City; Raleigh, NC; and Waco, TX.

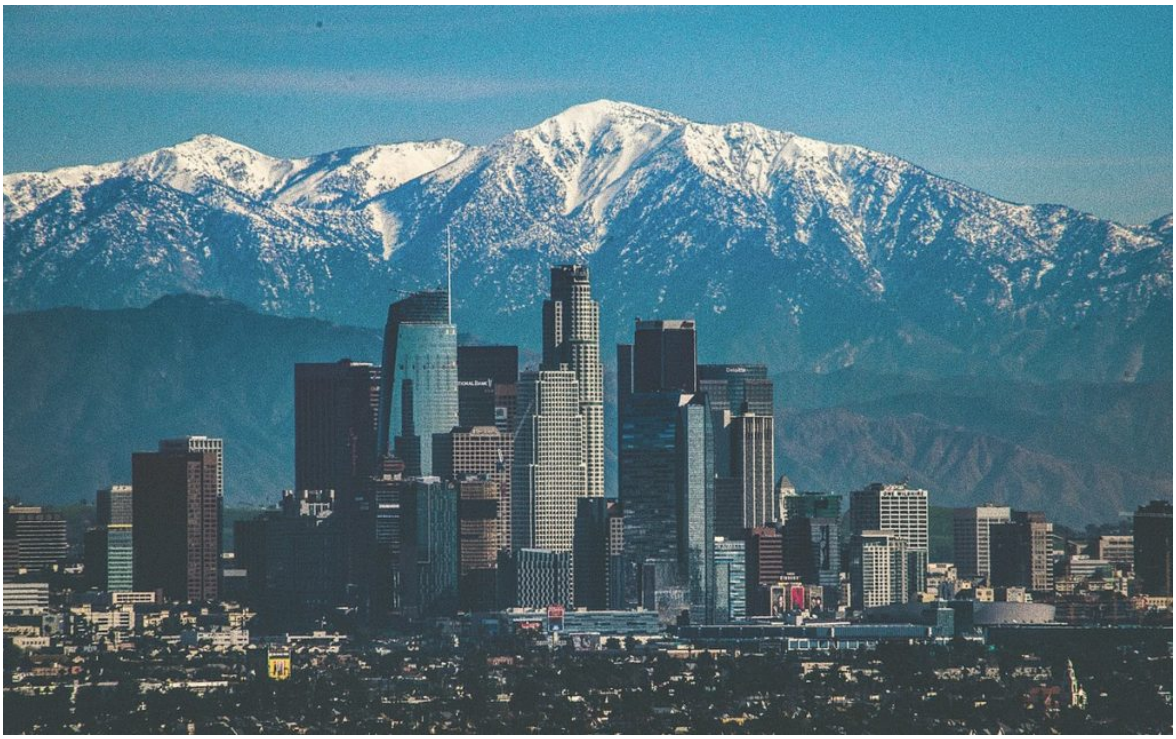
AT&T is making millimeter wave a focus of its 5G strategy to get better service in dense, urban areas where demand is already stretched. That makes the data transfer test significant — it shows that the carrier is moving ahead on the technology that would allow it to offer data beyond its spectrum holdings. The company is using Ericsson, Nokia and Samsung as its hardware suppliers, and said it has already started deploying infrastructure.

"We're at the dawn of something new that will define the next decade and generation of connectivity," said AT&T chief technology officer Andre Fuetsch in a statement. "Future smart factories and retailers, self-driving cars, untethered virtual and augmented realities, and other yet to be discovered experiences will grow up on tomorrow's 5G networks."

A key part of AT&T's launch strategy has also been to get into mid-sized cities in addition to large markets like Atlanta and Houston. In announcing Charlotte, Raleigh and Oklahoma City as 5G cities, AT&T said it was looking to "avoid a new digital divide" by getting new technology in smaller cities. The mix in the latest announcement

continues that trend, although AT&T notes that it will launch in “parts” of the cities, leaving open the possibility that neighborhoods already lacking connections could miss out on the initial 5G launch.

Read full story here…



AT&T And LA Explore Massive Public-Private Partnership To Impose Smart City Tech

Activists in Los Angeles should be hounding its city council day and night to stop these devilish negotiations to create the “smartest city” in America that would follow the China model of Technocracy. Public-Private Partnerships are a spawn of the United Nations and Sustainable Development, aka Technocracy. TN Editor

AT&T is exploring a public-private partnership (P3) that would make Los Angeles “one of the smartest cities in America.” Through the

partnership, AT&T would deploy Internet of Things (IoT) and small cell technology across the city to support a variety of smart systems.

Among the areas the two have discussed are digital kiosks, structural monitoring, digital infrastructure and emergency services, according to a release from AT&T. The company emphasized that it would offer connectivity to neighborhoods on the wrong side of the digital divide.

“Access to information is the foundation of equality, opportunity, and prosperity,” said Los Angeles Mayor Eric Garcetti in a statement. “We are establishing unique partnerships as we deploy new networks and technologies across L.A. — and we’re excited to be discussing with AT&T how to empower Angelenos with new tools that could make their lives easier and our communities stronger.”

P3s are catching on around the country as cities look to upgrade their technology, infrastructure and logistics. According to a recent survey from Black & Veatch, a global engineering, procurement, construction (EPC) and consulting company, more than 60% of respondents from cities and municipal organizations thought that P3s were an effective financing tool for smart cities, making it the most favored tool. Working with private companies can help cities defray the high up-front cost, while the governments offer a willing customer for companies on nascent technology.

U.S. Rep. Darrell Issa, R-CA, who co-chairs the Congressional Smart Cities Caucus, has talked up the need for P3s to keep the government from the “trailing edge of technology,” saying at a March event that partnerships were about “writing an authorization allowing others to innovate and giving them a way to monetize it.”

What Los Angeles and AT&T are exploring appears to be more than just a single project or system. AT&T would use its IoT and 5G technology throughout the city to support smart cities in a variety of arenas. AT&T, for example, said it is already using a small cell buildout to bring FirstNet communications to L.A.’s first responders. Los Angeles has been building out its capacity as a smart city, earning a gold-level What Works Cities certification from Bloomberg Philanthropies, and has tried

to innovate solutions to the city's notorious traffic problem.

Read full story here…

China Rebuffed: Australia Bans Huawei From Massive 5G Network Project

Since Huawei and the Chinese Technocracy are closely aligned, Australia has finally figured out that if allowed to participate in their 5G rollout, Huawei would be a direct conduit for espionage. China openly seeks to be the global leader in 5G technology. Huawei has long been suspected of spying for the government. TN Editor

Taking a page out of Trump's playbook – and coming at a tumultuous time for the country, with PM Turnbull apparently on his way out and the local government in disarray – Australia banned Chinese telecom giant Huawei Technologies from supplying equipment for a 5G mobile network, **citing risks of foreign interference and hacking which Beijing angrily dismissed as an "excuse" to tilt the playing field against a Chinese firm**.

The decision aligns Australia with the United States, which previously restricted Huawei and compatriot ZTE Corp from its own market for similar “security” reasons.

The surprising move – which has already antagonized Australia’s biggest trading partner – follows advice from security agencies, and signals a hardening of Australia’s stance toward its biggest export market as relations have soured over Canberra’s allegations of Chinese meddling in Australian politics.

In a statement on Thursday, the government said that national security regulations typically applied to telecom carriers would now be extended to equipment suppliers: “firms who are likely to be subject to extrajudicial directions from a foreign government” would leave the nation’s network vulnerable to unauthorized access or interference, and presented a security risk, the statement said according to Reuters.

Chinese law requires **organizations and citizens to support, assist and cooperate with intelligence work, which analysts say can make Huawei’s equipment a conduit for espionage.**

> *That’s what you get when you have the aligned strategy of a Chinese company with the Chinese government,” said John Watters, Executive Vice President and Chief Corporate Strategy Officer of cybersecurity firm FireEye Inc.*
>
> *“(Australia) basically made a decision to spend more money to have more control over their national communication system, because they’re up against a competitor that will sacrifice near-term margin for long-term intelligence advantage,” he said.*

While Australia did not identify the Chinese firm, an Australian government official said the order was aimed at Huawei and blocked its involvement in the network.

On Twitter, Huawei’s Australian arm, which has denied it is controlled by Beijing, said on Thursday that the action was an “extremely disappointing result for consumers”.

China, predictably, was furious with the announcement coming just months after the US engaged in a similar ban for security grounds. In Beijing, foreign ministry spokesman Lu Kang said China expressed "serious concern", adding that Australia should not "use various excuses to artificially erect barriers and conduct discriminatory practices". China also called the Australian decision wrong and said it should "not interfere" nor "restrict Chinese businesses from operating normally" for security purposes, an exclusion which apparently is only permitted for China.

- CHINA COMMERCE MINISTRY SAYS AUSTRALIA SHOULD NOT INTERFERE AND RESTRICT CHINESE BUSINESSES FROM OPERATING NORMALLY BASED ON THE GROUNDS OF NATIONAL SECURITY
- CHINA SAYS AUSTRALIAN GOVT.'S 5G DECISION IS `WRONG'

"We urge the Australian government to abandon ideological prejudices and provide a fair competitive environment for Chinese companies' operations in Australia," Lu said during the news briefing.

As Reuters notes, Australia had previously banned Huawei, the world's largest maker of telecommunications network gear, from providing equipment for its fiber-optic network and moved to block it from laying submarine cables in the Pacific. However, the latest Huawei exclusion from the mobile network comes at a time of particularly strained relations between Australia and China, **which Prime Minister Malcolm Turnbull had two weeks ago sought to reset with a conciliatory speech**.

Read full story here…