## NEG BLOCKS

### AT: AI Good

#### 1. The future of artificial intelligence is likely to be dominated by monopolies

**Stephen DeAngelis, 2015** (Stephen DeAngelis, president and CEO of the cognitive computing firm Enterra Solutions. February 2015. “The Upside of Artificial Intelligence Development,” *Wired*, <https://www.wired.com/insights/2015/02/the-upside-of-artificial-intelligence-development/>. Accessed 10/28/2016) ESG

\*\*\*Note: quoting Kevin Kelly, member of Global Business Network, a small think tank and consultancy based in Emeryville, California.

Unlike the dire warnings that have filled news outlets over the past year, Kelly’s view of the future of AI is not only optimistic it’s almost joyous. Wladawsky-Berger and Kelly are not alone in their optimism about AI’s future. Timothy B. Lee (@binarybits), senior editor at @voxdotcom, also believes that the up side of artificial intelligence will far outweigh the risks of developing it further. [“Will artificial intelligence destroy humanity? Here are 5 reasons not to worry.” Vox, 15 January 2015] Lee believes the naysayers “overestimate the likelihood that we’ll have computers as smart as human beings and exaggerate the danger that such computers would pose to the human race. In reality, the development of intelligent machines is likely to be a slow and gradual process, and computers with superhuman intelligence, if they ever exist, will need us at least as much as we need them.” Even though Kelly is optimistic about the future of AI, he doesn’t dismiss the cautions being raised about how it’s developed. He writes, “As AIs develop, we might have to engineer ways to prevent consciousness in them — our most premium AI services will be advertised as consciousness-free.” **Kelly’s big concern about AI’s future is who will control the systems we use. He explains: “Cloud-based AI will become an increasingly ingrained part of our everyday life. But it will come at a price. Cloud computing obeys the law of increasing returns, sometimes called the network effect, which holds that the value of a network increases much faster as it grows bigger.** The bigger the network, the more attractive it is to new users, which makes it even bigger, and thus more attractive, and so on. **A cloud that serves AI will obey the same law.** The more people who use an AI, the smarter it gets. The smarter it gets, the more people use it. The more people that use it, the smarter it gets. **Once a company enters this virtuous cycle, it tends to grow so big, so fast, that it overwhelms any upstart competitors. As a result, our AI future is likely to be ruled by an oligarchy of two or three large, general-purpose cloud-based commercial intelligences.”**

#### 2. AI allows mass scale surveillance/violation of privacy

Ryan Calo 2010 (Ryan Calo, Assistant Professor of Law at the University of Washington, 2010, European Journal of Legal Studies, “Peeping HALS: Making Sense of Artificial Intelligence and Privacy” <http://www.ejls.eu/6/83UK.htm> DoA: 10/14/16) CJV

Historically, AI can be said to threaten privacy according to a specific pattern: AI substitutes for humans at various stages of observation or surveillance, allowing such activity to reach a previously impracticable scale.   Whereas once telephonic surveillance required one listener per phone call, the development of voice recognition technology permits the substitution of a computer capable of monitoring thousands of calls simultaneously.[[6]](http://www.ejls.eu/6/83UK.htm" \l "_ftn6" \o ")  Whereas once hundreds of intelligence analysts might be required to pour over field records in search of connections, AI knowledge management techniques automatically spot patterns and call them to the attention of agents.[[7]](http://www.ejls.eu/6/83UK.htm" \l "_ftn7" \o ")  These developments vastly amplifying the potential for data gathering and analysis, and hence underpin ubiquitous surveillance.

### AT: Smart Grids

#### 1. The IoT increases security risks, which could create life and death scenarios for millions of people – the rising impact of data breaches is already apparent

**James Manyika et al, 2015** (James Manyika, director of the McKinsey Global Institute, Michael Chui, partner at MGI, Peter Bisson, global leader of the High Tech Practice at MGI, Jonathan Woetzel, Richard Dobbs, director at the MGI, Jacques Bughin, director at the MGI, and Dan Aharon, engagement manager at MGI. June 2015. “The Internet of Things: Mapping the Value Beyond the Hype,” *McKinsey Global Institute*, <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world>. Accessed 10/17/2016. Page 105) ESG

**The Internet of Things heightens existing concerns about cybersecurity and introduces new risks. It multiplies the normal risks associated with any data communication; each device increases the “surface area” available for breaches, and interoperability expands the potential scope of breaches.** Every node is a potential entry point, and interconnection can spread the damage. **Moreover, the consequences of compromised IoT systems that control the physical world could be catastrophic.** A compromised IoT-based home security system or a disrupted medical monitor could pose life-and-death risks. **A hacker attack on a smart grid system could potentially turn off power to millions of households and businesses, creating massive economic harm and threats to health and safety.** For individuals, IoT security breaches can involve both inappropriate use of personal data and theft (Exhibit 29). Mission-critical IoT applications (self-driving cars or military vehicles, for example) should have high levels of security before they are adopted on a large scale. And consumers will not accept applications such as touchless payment systems in retail unless they believe that their payment data are secure. It may be a hard sell: **according to the Identity Theft Resource Center, 2014 was a record year for data breaches, with reported incidents rising 27.5 percent from 2013.**

#### 2. Not only have Smart Grids been faulty, but they are worse for the consumer

**Lisa Margonelli 2010** (Lisa Margonelli, director of the New America Foundation’s Energy Productivity Initiative. November 19th 2010. “What’s Really Wrong With the Smart Grid,” *The Atlantic*, <http://www.theatlantic.com/national/archive/2010/11/whats-really-wrong-with-the-smart-grid/66832/>. Accessed November 18th 2016) ESG

Consumers, who are seeing their unspoken agreement with their utilities rewritten for the first time since the 1920's, have been left out of the discussion. Across the **country Smart Meters have become increasingly unpopular as they malfunction, overcharge customers, allow utilities to quickly disconnect homes, and put the burden of equipment installation on ratepayers**. (For detailed tracking see Jerry Richman's excellent blog.) While there's a tendency to see each bit of bad news as an isolated event, together I think they reflect a failure of the country's leaders to articulate a clear philosophy of the Smart Grid and its relationship to consumers. We really need to define the Smart Grid not in what it might offer interest groups, or why it's a "good idea," but in how it will empower consumers to save energy and money, encourage innovation in technology and markets, and create a stable atmosphere for investment and productive competition.

#### 3. Smart grids may increase consumption

**The Economist 2009** (The Economist, English-language weekly news magazine owned by the Economist Group. October 8th 2009. “Smart grids: Clever, but unprincipled,” *The Economist*, <http://www.economist.com/node/14587037>. Accessed November 18th 2016) ESG

That is partly because no one is quite sure what they are—and because “smart” sounds preferable to “dumb”. The term encompasses almost anything that would make power transmission more reliable, flexible and convenient, from meters that send in readings automatically to software that detects snapped cables and reroutes power supplies around them. The world's grids will certainly need some clever upgrades to manage the intermittent surges of electricity from the millions of wind turbines and solar panels that are planned to ward off the threat of global warming. If distributed generation (meaning small power sources such as rooftop solar arrays) becomes widespread, more sophisticated technology will be required to allow power to flow out from homes and offices as well as into them. That would also allow the batteries of electric cars to serve as a backup supply of power when needed. Technophiles imagine a time when smart grids will seamlessly balance supply and demand for power by turning down millions of air-conditioners a notch when the wind drops or the sun goes behind a cloud. Increasing the grid's IQ would bring more mundane benefits, too. Blackouts, which cost businesses billions each year, would become much rarer. Smarter meters could encourage conservation by letting customers know just how much power they are using, with which machines, at what cost, every minute of the day. Terrorists should find it harder to disrupt things. As Mr Obama put it when urging Congress to pass the stimulus bill, a smart grid “will save us money, protect our power sources from blackout or attack, and deliver clean, alternative forms of energy to every corner of our nation.” Spending lots of money on smart grids, however, will not bring about any of those things by itself. **The technology is not inherently frugal or green. It can be used to deliver not just clean renewable energy more efficiently, but also the grubby coal-fired sort. By reducing the need for expensive backup capacity, it may actually reduce the cost of electricity, and so encourage consumption.** The very fact that utilities and their customers, tree-huggers and industrialists alike are all keen on it hints at the many different ends to which it can be turned.

#### 4. Smart Grids can enable utilities to own and control your data

**Lisa Margonelli 2010** (Lisa Margonelli, director of the New America Foundation’s Energy Productivity Initiative. November 19th 2010. “What’s Really Wrong With the Smart Grid,” *The Atlantic*, <http://www.theatlantic.com/national/archive/2010/11/whats-really-wrong-with-the-smart-grid/66832/>. Accessed November 18th 2016) ESG

The chewier problem with the Smart Grid, as I see it, is **that your utility can profit from its knowledge of your habits by selling the electricity you're not using for a profit.** This isn't Corsi's jackbooted thugs busting down your doors, it's more like a boorish busybody sitting around your kitchen eying your plate and constantly saying, "Are you going to eat that?" The idea of my utility, or Google, making a profit from the energetic equivalent of my potato peelings is either the acme of boorishness or the highest attainment of the free market, depending upon how you look at it. And I think how we look at it will depend upon how successful the process is. If the Smart Grid brings us lower bills, lower carbon emissions, and better and more comfortable homes, without explicit invasions of privacy, we'll probably love it. But **if it fails to deliver on its promises, and becomes largely the tool of utilities to maximize profits and lock out competition, we will judge it a failure. Worse, if utilities or others sell information about our habits to third parties like health insurers who, for example, decide that we spend too much time in front of the TV drinking beer to be worth insuring, it will become a whole new problem.** This is another situation where the Obama administration needs to lead the alphabet soup of agencies overseeing the Smart Grid to clearly define a philosophy of consumer-centered privacy.

### AT: Reduced Emissions

#### 1. In spite of their claimed benefits, the data storage the Internet of Things requires produces more emissions

**Savitha Chinnadurai and Kiran Nandavarapu, 2015** (Savitha Chinnadurai, senior research analyst at WNS Global Services and Kiran Nandavarapu, ‎Director of Market and Competitive Intelligence at Blueocean Market Intelligence. November 23rd 2015. “Increasing Carbon Footprint of the ICT Sector,” *BlueOcean Market Intelligence*, <https://www.blueoceanmi.com/blueblog/increasing-carbon-footprint-of-the-ict-sector-2/>. 10/31/2016) ESG

According to SMART 2020 study, global greenhouse gas emissions will be cut by 15% by using low carbon generating ICT equipment. As product quantities grow and more devices are produced every year, this demands more connections. **In 2014, the Internet of Things (IoT) was estimated at 108 million ICT products and it is expected to grow by 23% by 2020.** Though **IoT products** help reduce the overall carbon footprint in other areas such as energy, transportation, built environments and agriculture, they **produce a great amount of data that needs storage, which leads to more carbon emissions.** In our next post, we will explore different initiatives and measures taken by various companies, associations and ICT vendors to reduce the overall carbon footprint.

#### 2. The IOT has a substantial energy footprint with more consumer electronics always, in a sense, being on

**Chris Mooney 2015** (Chris Mooney, reporter Washington Post. February 6, 2015. DOA: October 31, 2016. “Your home is full of devices that never turn off. And they’re costing you a lot of money,” Washington Post. <https://www.washingtonpost.com/news/energy-environment/wp/2015/02/06/your-home-is-full-of-devices-that-never-turn-off-and-theyre-costing-you-a-lot-of-money/?utm_term=.4cb036df9fba>) EL

And the MEL problem is getting worse, for at least two separate reasons. The first reason is actually kind of good news — major home appliances aren’t such power hogs any more. Many categories of in-home appliances, such as refrigerators, have gotten vastly more energy efficient over time: These energy efficiency strides are a powerful achievement, but they also leave behind the “miscellaneous electrical load” as a category of energy use that is increasing — both overall, and especially in relation to other categories. The second problem, explains Meier, is that **we’ve got more and more consumer electronic devices, and they are performing more and more wireless communications that require them to be, in some sense, always “on.” “A lot more devices have network connections, so that they’re constantly talking to the Internet in one way or another,”** says Meier. **The “**[**Internet of Things**](http://share.cisco.com/internet-of-things.html)**,” it seems, has a substantial energy footprint.**

#### 3. The Internet of Things increases material and energy consumption

**Klint Finley, 2014** (Klint Finley, writer for *Wired Business*. June 5th 2014. “The Internet of Things Could Drown Our Environment in Gadgets,” <https://www.wired.com/2014/06/green-iot/>. Accessed 10/31/2016) ESG

But **this vast network of new online devices could also end up harming the environment. Manufacturing all those gadgets means expending both energy and raw materials. In many cases, they will replace an older breed of devices, which will need to be disposed of** (so long, non-smart thermostat). **And eventually, every IoT device you buy–and people are predicting there will be hundreds of thousands–will need to be retired too.** Since all these devices will connect to the net, we should even consider the energy used by the data centers that drive them. “The Internet of Things, for us, is a way for people to get reconnected with where their energy comes from,” **says Greenpeace IT analyst Gary Cook. “But it could also drive more consumption, which won’t help us.”**

#### 4. In the long run, we’ll see a substantial increase in e-waste

**Bonnie Gardiner, 2014** (Bonnie Gardiner, journalist at *ComputerWorld*. December 8th 2014. “The hidden environmental cost of the Internet of Things,” *ComputerWorld*, <http://www.computerworld.com.au/article/561064/hidden-environmental-cost-internet-things/>. Accessed 10/31/2016) ESG

\*\*\*Note: EOL = end-of-life for a product

**Analyst firm Gartner is forecasting that the IoT will encompass some 30 billion connected devices by 2020.** And while networking vendor Cisco has pegged the IoT's value at $14.4 trillion between 2013 and 2022, questions are being asked over its potential environment cost. What becomes of these thousands of sensors and smart devices once they reach EOL? Bettina Tratz-Ryan, research VP and green IT specialist with Gartner, says that this is one of her biggest concerns around the growth of the IoT. “Gartner has forecast that by 2020 we will have 26 billion items deployed in the world; **what happens to these sensors, once they go into the waste bin?**" the analyst asks. "Are they ending up in landfills? **If they’re embedded in these objects and technologies, it’s almost impossible to recycle them.**" Australians already generate more than 140,000 tonnes of e-waste each year, according to City of Sydney. **On a global scale, the United Nations University (UNU) estimates that in 2013, 53 million tonnes of e-waste were disposed of worldwide, while around 67 million tonnes of new electrical and electronic equipment were put on the market. The Stopping the E-waste Problem (StEP) initiative**, a joint effort from UN organisations, grassroots groups and industry, **predicts that by 2017 the total annual volume of e-waste will have risen by a third, to 65.4 million tonnes — almost 11 times the weight of the Great Pyramid of Giza.**

#### 5. The rebound effect leads to a net increase in emissions

**Runar Brannlund et al 2005** (Professor at the Department of Economics, Umea˚ University, SE-901 87 Umea˚, Sweden. October 24, 2016. “Increased energy efficiency and the rebound effect: Effects on consumption and emissions,” *Science Direct*. <https://www.researchgate.net/publication/4944399_Increased_Energy_Efficiency_and_the_Rebound_Effect_Effects_on_Consumption_and_Emissions> PAGE: 1 DOA: 11/20/16) CDY

The main objective of this paper is to examine how exogenous technological progress, in terms of an increase in energy efficiency, affects consumption choice by Swedish households and thereby emissions of carbon dioxide (CO2), sulphur dioxide (SO2) and nitrogen oxide (NOx). The aim of the paper is closely related to the discussion of what is termed the brebound effectQ. To neutralise the rebound effect, we estimate the necessary change in CO2 tax, i.e. the CO2 tax that keeps CO2 emissions at their initial level. In addition, we estimate how this will affect emissions of sulphur dioxide and nitrogen oxides. **The** **results indicate that an increase in energy efficiency of 20% will increase emissions of CO2 by approximately 5%.** To reduce the CO2 emissions to their initial level, the CO2 tax must be raised by 130%. This tax increase will reduce the emissions of sulphur dioxide to below their initial level, but will leave the emissions of nitrogen oxides at a higher level than initially. Thus, if marginal damages from sulphur dioxide and nitrogen dioxide are non-constant, additional policy instruments are needed. D 2006 Published by Elsevier B.V.

#### 6. Energy conservation progress is slowing because of fears from IT managers

**Patrick Thibodeau 2014** (Patrick Thibodeau, senior editor at Computerworld. August 6, 2014. DOA: November 5, 2016. “Data centers are the new polluters,” Computerworld. <http://www.computerworld.com/article/2598562/data-center/data-centers-are-the-new-polluters.html>) EL

The report also finds that **energy efficiency progress is slowing. Once the obvious efficiency projects**, **such as isolating hot and cold aisles, are completed, additional investment in energy efficiency becomes harder to justify -- either because of the cost or because of a perception that new initiatives might increase risk.** **IT managers are "extremely cautious" about implementing aggressive energy management programs** because they're concerned that such measures could threaten uptime, the report notes.

#### 7. Democracy is key to environmental protectionism

**Quan Li and Rafael Reuveny, 2006** (Quan Li, professor of political science at Texas A&M University, and Rafael Reuveny, professor in Indiana University Bloomington’s School of Public and Environmental Affairs. 2006. “Democracy and Environmental Degradation,” *International Studies Quarterly*, <http://people.tamu.edu/~quanli/papers/ISQ_2006_demenv.PDF>. Accessed November 16th 2016. Page 935) ESG

In a relatively small but growing body of literature in political science and environmental studies, scholars debate the effect of democracy on environmental degradation. Some theorists claim that democracy reduces environmental degradation. Others argue that democracy may not reduce environmental degradation or may even harm the environment. Empirical evidence thus far has been limited and conflicting. This article seeks to address the democracy–environment debate. We focus on the effect of political regime type on human activities that directly damage the environment. Our discussion of the theoretical literature identifies different causal mechanisms through which democracy could affect environmental degradation. The empirical analysis focuses on the net effect of these competing mechanisms. **We examine statistically the effect of democracy on five aspects of human-induced environmental degradation–carbon dioxide emissions, nitrogen dioxide emissions, deforestation, land degradation, and organic pollution in water. We find that democracy reduces all five types of environmental degradation.** While the substantive effect of democracy is considerable, it varies in size across different types of environmental degradation. We also find nonmonotonic effects of democracy that vary across the environmental indicators.

### AT: Smart Cities

#### 1. Smart infrastructure could be harmfully tampered with

**Bob Graves, 2015** (Bob Graves, associate director of the Governing Institute who presents on smart and sustainable approaches to water, waste, energy, transportation and building systems drawing from his more than 25 years of experience. August 26th 2015. “How Secure is Smart Infrastructure?” *Government Technology*, <http://www.govtech.com/security/How-Secure-Is-Smart-Infrastructure.html>) ESG

**A chief concern is that sensors can intentionally be fed bad data that leads to faulty analysis and action. Automated elevators, lighting and building security systems, for example, could be disrupted. Roadway sensors connected to a smart traffic light system could be hacked and used to bring vehicle movement in a city to a halt. One needn't look any further than the impact of last winter's snowstorms on cities like Boston to see how this could disrupt businesses, schools and emergency services. Potential outcomes like these raise important governance issues.** "Who's responsible when a smart city crashes?" futurist Simon Moores asked during his keynote session at a recent conference in London. That question might be glibly answered with "the mayor" or "the city manager," but these responses are at best inadequate. Unlike during a severe snowstorm, **the cause of such a debacle would be invisible and a mayor or city manager would be unable to mobilize an immediate solution.** "Integrating an entire city full of these networks," Moores elaborated, "presents an almost intractable problem with two really, really big challenges: security and a lack of standards." While these challenges might call into question the open design of the Internet, there's little chance of changing its basic framework. What will be needed instead are new regulations and standards to enable disparate systems to be securely connected.

#### 2. This is likely inevitable

**Steven Poole, 2014** (Steven Poole, reporter for *the Guardian*. December 17th 2014. “The truth about smart cities: ‘In the end, they will destroy democracy',” *The Guardian: Cities* *[supported by the Rockefeller Foundation],* <http://www.theguardian.com/cities/2014/dec/17/truth-smart-city-destroy-democracy-urban-thinkers-buzzphrase>) ESG

What’s more, if an entire city has an “operating system”, what happens when it goes wrong? **The one thing that is certain about software is that it crashes.** The smart city, according to Hollis, is really just a “perpetual beta city”. **We can be sure that accidents will happen** – driverless cars will crash; bugs will take down whole transport subsystems or the electricity grid; drones could hit passenger aircraft. How smart will the architects of the smart city look then?

#### 3. Smart cities will be used for surveillance, and private companies don’t have gov’t accountability

**Allegra Kirkland, 2015** (Allegra Kirkland, AlterNet's associate managing editor. March 1st 2015. “The Terrifying ‘Smart’ City of the Future,” *Alternet*, <http://www.alternet.org/civil-liberties/terrifying-smart-city-future>) ESG

Smart cities are loosely defined as urban centers that rely on digital technology to enhance efficiency and reduce resource consumption. This happens by means of ubiquitous wireless broadband, citywide networks of computerized sensors that measure human activities (from traffic to electricity use), and mass data collection that analyzes these patterns. Many American cities, including New York, Boston and Chicago, already make use of smart technologies. But far more radical advances are happening overseas. Masdar, in Abu Dhabi, and Songdo, in South Korea, will be the first fully functioning [5] smart cities, in which everything from security to electricity to parking is monitored by sensors and controlled by a central city “brain.” **The surveillance implications of these sorts of mass data-generating civic projects are unnerving, to say the least. Urban designer and author Adam Greenfield wrote** on his blog Speedbird **that this centralized governing model is “disturbingly consonant with the exercise of authoritarianism.” To further complicate matters, the vast majority of smart-city technology is designed by IT-systems giants like IBM and Siemens.** In places like Songdo, which was the brainchild [7] of Cisco Systems, **corporate entities become responsible for designing and maintaining the basic functions of urban life.** Smart cities are predicated on the neoliberal idea that the market can fix anything—that companies can manage cities better than governments can. Their advocates claim that they will enhance democratic participation by relying on crowdsourcing and “civic hacking projects [8]” that allow locals to use newly available data to solve municipal problems. But they ignore the fact that **private corporations are the ones measuring and controlling these mountains of data, and that they don’t have the same accountability to the public that government does.**

### AT: Connected Cars

#### 1. Connected cars are vulnerable to cyber attacks which leads to safety hazards and financial damage

Mark Lengton et al., 2015. (Mark Lengton, Diederik Verzijl & Kristina Dervojeda, a Senior Consultant at PricewaterhouseCoopers, a consulting firm. February 2015. “Connected Cars,” *Commissioned by the European Union*, <file:///Users/dibarra20/Downloads/43-iot-connected-cars_en.pdf> . Accessed on 10/27/16. 12.) DIB

Connected cars are potentially very vulnerable to cybercrime. In fact, researchers have already shown that malicious input can be delivered through compromised MP3s, infecting a whole network of cars in a near instant. This can cause both financial damages and safety hazards to the users of connected cars, e.g. by turning off vital functionalities of the car that jeopardize the safety of drivers or by compromising credit card information stored by connected car services.

#### 2. Connected cars are high risk, low reward

**Jonathan Gitlin, 2016** (Jonathan Gitlin, scholar at the University of Kentucky’s Technology Policy at the Patterson School of Diplomacy and International Relations. May 7th 2016. “The connected car may be the dumbest idea ever, but it’s not going away,” *ArsTechnica,* <http://arstechnica.com/cars/2016/05/its-time-for-a-candid-talk-about-connected-cars/>. Accessed November 18th 2016) ESG

There's just one problem: most Ars readers, in my experience, think connecting a car to the internet is the dumbest thing you can do on four wheels. Who can blame them? **Last year saw a litany of car hacks that affected aftermarket devices but also security flaws direct from the factory**—1.4 million Fiat Chrysler vehicles had to be recalled as a result. The problem is with the digital nervous system of our cars. Back when automotive network standards were being created, the idea that cars would use the Internet to interface with the outside world was ludicrous. And so, there's little—or none—of the sort of network security in place that you'd take for given if designing things from a clean sheet. **As long as you have access to the Connected Area Network (or CAN), your electronic hooks are into the engine, the brakes, and even the steering. And for what?** Having tested a bunch of consumer connected car products, from Automatic through to Zubie, **I struggle to see the benefit. You can quantify your driving, but by and large these gadgets amount to a Fitbit for your car. I don't know about you, but I'm not sure my car needed a Fitbit in the first place.**

#### 3. Autonomous cars can’t make complex decisions

**Andrew Ng and Yuanqing Lin, 2016** (Andrew Ng, Chief Scientist at Baidu Research in Silicon Valley, and Yuanqing Lin, director of the Baidu Institute of Deep Learning, and the Deputy General Manager of the Baidu Autonomous Driving Business Unit. March 15th 2016. “Self-Driving Cars Won’t Work Until We Change Our Roads–And Attitudes,” *Wired*, <https://www.wired.com/2016/03/self-driving-cars-wont-work-change-roads-attitudes/>. Accessed November 18th 2016) ESG

Today’s autonomous cars are inferior to human drivers in important ways: **If a construction worker uses hand gestures to tell a car to either go or to stop, no autonomous car today can reliably make the right decision. When the sun is immediately behind a traffic light, most cameras won’t be able to recognize the color of the signal through the glare**. If we see a truck with a “Makes Wide Turns” sign, we know how to adjust our driving accordingly. If we see children distracted by the ice cream truck across the street, we know to slow down, as they may dash toward it. **Today’s computers aren’t nearly as skilled at interpreting complex situations like these.**

#### 4. Connected cars might emit more ☹

**Alex Davies, 2016** (Alex Davies, transportation writer for *Wired*. November 18th 2016. “So, Nobody Knows How Much Self-Driving Cars Will Pollute,” *Wired*, <https://www.wired.com/2016/11/nobody-knows-much-self-driving-cars-will-pollute/>. Accessed November 19th 2016) ESG

The problem is that nobody knows how these vehicles will be used, especially in the early years. You could assume that because the tech will likely debut via ride-sharing services, people will need fewer cars, and so cars will drive fewer overall miles. Or, **because riding in a car gets way nicer when you don’t have to do anything, vehicle miles might soar**. Smarter cars could drive more closely together, but that will require a critical mass of autonomous cars on the road—a threshold that’s decades away. Shared cars could spend lots of time “deadheading”—driving around empty between pickups, but that might actually improve emissions, since they’d be running constantly, and warm engines are cleaner than cold ones.

#### 5. The cost of IoT is too high for it to be widely implemented

**Tim Brugger, 2016** (Tim Brugger, freelance writer at Quality Content LLC and *Business Insider*. February 4th 2016. “Consumers aren’t ready for an Internet of Things world,” *Business Insider*, <http://www.businessinsider.com/internet-of-things-world-may-be-too-pricy-2016-2?pundits_only=0&get_all_comments=1&no_reply_filter=1>. Accessed Nov 15 2016) ESG

With so much discussion surrounding the IoT, it's not surprising that folks around the globe recognize the impact it will eventually have on our day-to-day lives. But from a consumer's perspective, understanding the upside of smart homes, cars, and cities is one thing — actually purchasing and implementing IoT devices is another matter. **The No. 1 roadblock to consumers purchasing an IoT device today is price. As often happens when new technologies are introduced to the masses, the initial costs are prohibitive for most people. According to the Accenture data, in a worldwide survey of Internet users, 62% said IoT "things" were too expensive** with Alphabet's Nest smart home hub as just one example. Smart home devices — along with smart cars — are expected to be the entrée for the general public into the realm of IoT, which is great news for Alphabet and its IoT home-technology division, Nest. But **the asking price of around $200 for a smart thermostat or WiFi home-security camera is more than most consumers are willing to shell out.**

### AT: Big Data Good

#### 1. **Big data takes away our autonomy by tracking us**

Julia Powles 2015 (Julia Powles,legal academic working on technology law and policy at the [University of Cambridge](http://www.law.cam.ac.uk/people/academic/j-powles/4273) and a former contributing editor and policy fellow of the Guardian. 15 July 2015 “Internet of things: the greatest mass surveillance infrastructure ever?” from The Guardian. <https://www.theguardian.com/technology/2015/jul/15/internet-of-things-mass-surveillance> DOA: 10/25/16) ESM

And the reason we ought to accept this unpalatable, feudal state of affairs? The lures of big data, and the venerated openness of the network. Your toaster is hackable, yes (as may be the rest of these smoking guns in your city), but at the same time, in a nebulous trade-off, with “dictators dying off and the data trail of bad behaviour growing, the biggest dirty networks are on the brink of collapse”. And when the “modern state fails, the internet of things will provide governance”, Howard asserts, unconvincingly. By [tracking us](https://www.theguardian.com/technology/2015/may/25/forget-internet-of-things-people) in intensive and intrusive ways – not only in our homes, but in our vehicles and [bodies](http://www.slate.com/articles/technology/future_tense/2015/03/implanted_medical_devices_and_security_in_nigeria.html) – data-driven devices can [nudge, manipulate and mould](https://www.theguardian.com/technology/2014/jul/20/rise-of-data-death-of-politics-evgeny-morozov-algorithmic-regulation) our behaviours, habits and preferences, limit our autonomy, and bring quantification, segregation and discrimination to what is currently a political economy held together by social fuzziness. This fuzziness assists us individually – because we have [control over](https://www.theguardian.com/technology/2015/may/07/surveillance-privacy-philosophy-data-internet-things) who has, and importantly [who does not have](https://www.theguardian.com/technology/2015/apr/06/data-privacy-europe-facebook), personal information about us. But it is also important socially, unless we want to turn into an intensely individualistic, segmented, micro-financialised network of semi-autonomous, tethered beings. We deserve a smarter solution that offers more than empty marketing rhetoric for “open”, “inclusive” monopolistic big tech business models. At worst, it’s a terrifying blueprint for the [end of politics](http://www.thedailybeast.com/articles/2015/02/13/stop-demonizing-the-internet.html), depoliticising our engagement with “things”, [characterising the objects](https://www.youtube.com/watch?v=lHTthJlYokM) and relations that furnish our lives as “[loss leaders for data flows](https://www.youtube.com/watch?v=lHTthJlYokM)” – data flows that offer nothing for us, and everything for a staggering, uncontrolled array of corporate and governmental actors.

#### 2. Big Data means discrimination in the workplace because of analysis algorithms used on data

**Scott Pepett 2014** (Scott R. Pepett, Professor of Law in University of Colorado, March 1st , 2014, “Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security &amp; Consent”, Social Science Research Network, http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=2409074, Accessed 10-28-2016, Page 117) SEO

The first Internet of Things problem is the Achilles’ heel of widespread sensor deployment: **Internet of Things data will allow us to sort consumers more precisely than ever before, but such sorting can easily turn from relatively benign differentiation into new and invidious types of unwanted discrimination**. This subpart explores both the technical and legal problems of discrimination on the Internet of Things. The technical problem is simple: **coupled with Big Data or machine learning analysis, massive amounts of sensor data from Internet of Things devices can give rise to unexpected inferences about individual consumers. Employers, insurers, lenders, and others may then make economically important decisions based on those inferences, without consumers or regulators having much understanding of that process.** **This could lead to new forms of illegal discrimination** against those in protected classes such as race, age, or gender. More likely, it may create troublesome but hidden forms of economic discrimination based on Internet of Things data. Currently, both traditional discrimination law and information privacy law, such as the FCRA, are unprepared for such new forms of discriminatory decision making.

### AT: Helps Businesses

#### 1. 75% of organizations in the last year have been hacked and 60% of small companies don’t survive cyber attacks

Gary Miller Oct 2016 (Gary Miller, from GEM strategy management writing in the Denver Post; 10/23/16; “60% of small companies that suffer a cyber attack are out of business within six months”; DOA: 11/5/16; <http://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/> ) AM

**The U.S’ National Cyber Security Alliance found that 60 percent of small companies are unable to sustain their businesses over six months after a cyber attack.** According to the Ponemon Institute, **the average price for small businesses to clean up after their businesses have been hacked stands at $690,000; and, for middle market companies, it’s over $1 million. Recent events have proven that nobody is safe from the threat of cybercrime – not large corporations, small businesses, startups, government agencies** or even presidential candidates. Small and mid-sized **businesses are hit by 62 percent of all cyber-attacks, about 4,000 per day, according to IBM**. Cybercriminals target small businesses because **they are an easy, soft target** to penetrate. They steal information to rob bank accounts via wire transfers; steal customers’ personal identity information; file for fraudulent tax refunds; and, commit health insurance or Medicare fraud. So what can you do besides pray and hope you’re not next? Remember, most cyber breaches happen because an employee does something that they aren’t supposed to do. Basic training can stop a majority of low-level threats. But, coaching your employees on data protection is not enough. Business owners must establish data security protocols, policies, practices and procedure that every employee takes seriously. Create a business continuity and incident response plan. This will be put into effect immediately once you know your systems have been compromised. Keep security software current. Having the latest security software, web browser and operating systems are the best defenses against viruses, malware and other online threats. When in doubt, delete it. Links in e-mails, tweets, posts and online advertising are often how cybercriminals try to steal information. Even if you know the source, if something looks suspicious, delete it. Protect all devices that connect to the Internet. Along with computers, smartphones, tablets, and other web-enabled devices need to be protected from viruses and malware. Plug and scan. USBs and other external devices can be infected by viruses and malware. Use your security software to scan them. Consider cyber insurance. While premiums continue to rise, the cost of the insurance will look small in comparison to the cost of experts and consultants to restore your systems — or the cost going out of business. Expand beyond IT. Don’t delegate cyber-crime prevention solely to your IT department and tell them “get on with it.” Embed these practices across all areas of your business. Encrypt your most sensitive files. Encrypting data is a process of converting data into a form, where it becomes unintelligible to any person without access to a key/password to decrypt the data. Encryption may be hardware or software based. Hardware encryption and decryption processes are executed by a dedicated processor on the hardware encrypted device. In software encryption, the resources of the device on which the software is installed are used to encrypt and decrypt the data. Robert Fleming, founder and president of Blacksquare Technologies, a Denver manufacturer of the Enigma hardware encryption device, said hardware encryption is faster. “The cryptographic key is stored in a separate, inaccessible portion of memory storage or stored off site, thus making it more secure than software encryption. Even if a company is hacked, and the bad guys capture your files, they cannot open any files that are encrypted”. Websites hacked. Corporate data leaked. Identities stolen. The threats are real and growing. **Small business owners have to assume they will be victims of cybercriminals since 75 percent of all organizations have experienced a data/cyber security breach in the past 12 months** and 82 percent of all Social Security numbers have been hacked more than once. **Cybercrime is now the world’s largest business** running in the trillions of dollars. So far **the “bad guys” are winning**. So business owners need to do more than hope and pray that their businesses won’t be next.

#### 2. DDoS attacks create significant financial costs

**Ian Barker, 2015** (Ian Barker, freelance technology writer with a history of work in technical support. 2015. “DDoS attacks are more dangerous than you think,” *BetaNews*, <http://betanews.com/2015/09/18/ddos-attacks-are-more-dangerous-than-you-think/>. Accessed 10/28/2016) ESG

We all know that DDoS attacks are capable of causing massive inconvenience, but according to a new survey they can have major financial and data loss implications too. The study of over 5,000 companies by Kaspersky Lab finds that almost one in three DDoS attacks coincides with a network intrusion. According to the research, 20 percent of businesses with 50 or more employees have suffered at least one DDoS attack. Furthermore, over a quarter of attacks lead to the loss of sensitive data, an unexpected and damaging consequence of a DDoS attack. Small businesses are most likely to lose data as a result of a DDoS attack -- 31 percent of SMBs reported data loss compared with 22 percent of larger enterprises. **There's a financial cost too. On average, a DDoS attack costs SMBs more than $50K in recovery bills, which is significantly more than the typical costs they face recovering from other types of attack. Larger enterprises spend a lot to recover from a third-party failure or cyber espionage attack, but a typical financial loss for enterprises from a DDoS attack is $417,000**, below average compared to recovery from other types of attacks.

#### 3. Cybercrime costs up to 65 million for businesses

**Ponemon Institute 2015** (Ponemon Institute, October 2015, Sponsored by Hewlett Packard Enterprise, Hewlett Packard, " 2015 Cost of Cyber Crime Study: Global", http://www.ponemon.org/blog/2015-cost-of-data-breach-global, Accessed: 11/11/16) SEO

As shown in Figure 3, **the total annualized cost of cyber crime in 2015 ranges from a low of $.31 million to a high of $65 million**. The median annualized cost of cyber crime in the benchmark sample is $5.5 million – a slight decrease from $6 million in 2014. **The mean value is $7.7 million**. A slight increase from last year’s mean of $7.6 million. The percentage net change from last year’s mean for seven countries is 1.9 percent.

### AT: Economic Benefits

#### 1. IoT will cause mass disruption in labor markets–including trucking unemployment which could be disastrous–IoT hurts poor with losing jobs

Sean Illing, 2016 (Sean Illing, Interviews Writer for Vox, taught politics and philosophy at Louisiana State University, paramedic in the United States Air Force. Oct 17, 2016. “Why we need to plan for a future without jobs: Andy Stern spent his career organizing workers. Here’s why he thinks work is doomed.,” *Vox*, <http://www.vox.com/conversations/2016/10/17/13245808/andy-stern-work-universal-basic-income-technology-artificial-intelligence-unions>. DOA: 10/24/16.) NB

The reason it's necessary is we're now learning through lots of reputable research that technological change is accelerating, and that this process will continue to displace workers and terminate careers. A significant number of tasks now performed by humans will be performed by machines and artificial intelligence. We could very well see 5 million jobs eliminated by the end of the decade because of technology. We’ve already seen Uber-deployed driverless cars in Pittsburgh, and driverless trucks will be deployed in the next five to six years — we’ve already seen them across Europe. The largest job in 29 states is driving a truck. There are 3 and a half million people who operate trucks and 5 million more who support them in various ways.

#### 2. IoT accelerates the replacement of labor with capital which only accelerates economic inequality, thus benefits of IoT accrue at the top, as bottom loses jobs

Sean Illing, 2016 (Sean Illing, Interviews Writer for Vox, taught politics and philosophy at Louisiana State University, paramedic in the United States Air Force. Oct 17, 2016. “Why we need to plan for a future without jobs: Andy Stern spent his career organizing workers. Here’s why he thinks work is doomed.,” *Vox*, <http://www.vox.com/conversations/2016/10/17/13245808/andy-stern-work-universal-basic-income-technology-artificial-intelligence-unions>. DOA: 10/24/16.) NB

Andy Stern I don’t see it now because I think no one wants to admit what’s happening. No one wants to admit that our half-measures aren’t working and won’t work. I think people completely underestimate the speed at which these changes are occurring. Sean Illing If we don’t implement something like a UBI, what does work and the middle class look like in 30 years? Andy Stern It looks like the Hunger Games. It’s more of what we’re beginning to see now: an enclave of extremely successful people at the center and then everyone else on the margins. There will be fewer opportunities in a hollowed out and increasingly zero-sum economy. If capital trumps labor, the people who own will keep getting wealthier and the people who supply labor will become less necessary. And this is exactly what AI and robotics and software are now doing: substituting capital for labor.

#### 3. Furthermore, security risks cost households BILLIONS

Britton 2016 (Katherine Britton , is an attorney in Dallas,TX and is a Certified Information Privacy Professional (CIPP/US) through the International Association of Privacy Professionals April 2016. “Handling Privacy and Security in the Internet of Things” from JOURNAL OF INTERNET LAW. PDF. DOA: 10/20/16 p. 4) ESM

Consumers’ abilities to prevent malware attacks currently are low. An independent study by the trusted Consumers Union, publisher of Consumer Reports magazine in 2011 revealed that one-third of households in the United States have experienced a malicious software infection in the previous year, costing consumers $2.3 billion annually.6 While there are obvious consumer benefits to connected devices, they add tremendous complexity and vulnerabilities that can be exploited. The growing complexity of computer software have direct implications for security. Complexities can be considered by examining the number of lines of computer code required for a piece of software or system function. It takes 45 million lines of code (LOC), for example, for Microsoft Office 2013 to function. That is slightly fewer than the 50 million LOC required to run the Large Hadon Collider located at the European Organization for Nuclear Research. Today, the software required to run the aver- age modern automobile is a remarkable 100 million LOC, many fewer than the unprecedented reported 500 million LOC that ran the US Healthcare.gov Web site.7

#### 4. DDoS attacks cost even more

**Ponemon Institute 2012.**(Ponemon Institute, independent researcher on privacy, data protection and information security policy. November 2012. DOA: November 4, 2016.“Cyber Security on the Offense: A Study of IT Security Experts,” Ponemon Institute. <https://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/CyberSecurityontheOffense.pdf> Page: 2) EL

As cyber attacks grow in sophistication and stealth, organizations are urged to be proactive in addressing the threats. As revealed in this research, a major consequence of not preventing attacks such as DDoS (denial of service) can be costly. **On average DDoS attacks are costing companies approximately $3.5 million annually,** according to the findings of this research.1

### AT: Health Benefits

#### 1. Data in healthcare is weak and inaccurate

**Kristen Lee, 2015** (Kristen Lee, news writer for *SearchHealthIT*. July 2015. “Barriers to conquer before IoT in healthcare helps Mrs. Smith,” *IoT Agenda*, <http://internetofthingsagenda.techtarget.com/feature/Barriers-to-conquer-before-IoT-in-healthcare-helps-Mrs-Smith>. Accessed 10/31/2016) ESG

\*\*\*Note: Shrestha = Rasu Shrestha, M.D., chief innovation officer at the University of Pittsburgh Medical Center (UPMC)

**Poor data accuracy defies IoT in healthcare** From Shrestha's seat, workflow is one of many challenges ahead before healthcare IoT can be fully realized. **Poor data management is one of those obstacles.** "Today [there] isn't really that much of a standard around how data is being captured, and **the accuracy of the information … may not be as accurate as we might hope for it to be."** **Furthermore, lack of interoperability only adds more barriers to capturing data and making sure information is accurate. With dozens, if not hundreds, of different device manufacturers** -- all of which may have different standards and communication capabilities -- **it is a challenge ensuring that these devices can "talk to each other,"** Shrestha said. And it's not only a matter of simply talking to each other, but also sending "the right messages in the way that the smart grids and the networks that we're trying to create would actually understand and have that level of interoperability," Shrestha said.

#### 2. Medical technology currently fails

**Robert Wachter, 2015** (Robert Wachter, Professor in the Department of Medicine at the University of California, San Francisco. March 21st 2015. “Why Health Care Tech is Still So Bad,” *The New York Times*, <http://www.nytimes.com/2015/03/22/opinion/sunday/why-health-care-tech-is-still-so-bad.html>. Accessed Nov 10th 2016) ESG

**Even in preventing medical mistakes** — a central rationale for computerization — **technology has let us down. A recent study of more than one million medication errors reported to a national database between 2003 and 2010 found that 6 percent were related to the computerized prescribing system.** At my own hospital, in 2013 we gave a teenager a 39-fold overdose of a common antibiotic. The initial glitch was innocent enough: A doctor failed to recognize that a screen was set on “milligrams per kilogram” rather than just “milligrams.” But the jaw-dropping part of the error involved alerts that were ignored by both physician and pharmacist. The error caused a grand mal seizure that sent the boy to the I.C.U. and nearly killed him. How could they do such a thing? **It’s because providers receive tens of thousands of such alerts each month, a vast majority of them false alarms. In one month, the electronic monitors in our five intensive care units, which track things like heart rate and oxygen level, produced more than 2.5 million alerts. It’s little wonder that health care providers have grown numb to them.**

#### 3. Healthcare IoT can be hacked and can kill

**Hailey Carlson, 2016** (Hailey Carlson, reporter for Axiom Cyber Solutions. October 28th 2016. “The Internet of Things Security: Hacking Healthcare,” *Axiom Cyber Solutions*, <https://www.axiomcyber.com/blog/internet-of-things-iot/iot-security-hacking-healthcare/>. Accessed Nov 10th 2016) ESG

Car hacking is not the only real-world, physical threat driven by IoT, as the healthcare industry has found a few IoT-related vulnerabilities of its own. As more and more modern medical devices are being developed, they are adding to the collection of connected devices encompassed by IoT; however, **many healthcare professionals have found that with these more advanced devices, comes more advanced cyber-threats as well.** One of the most recent and notable of these is the threat to Johnson & Johnson’s Animas One Touch Ping insulin pump. This insulin pump is special in that it is equipped with a remote control so that users do not need to remove their clothing to give themselves a dose of insulin. The problem with this is that the wireless connection between the remote and the pump is unencrypted, and consequently, highly vulnerable. Because of this, the pump can be hacked within a 25-foot radius of the user, and with the right radio equipment, a hacker can take control of the pump and trigger unauthorized insulin injections. **Not only does this threaten a specific device, but in some cases, it gives hackers access to the entire hospitals’ system. Similar to the car hacking instance, this not only poses immediate cyber-threats, but it could have deadly repercussions**, as different diabetes patients need varying levels of insulin at different times. **A malicious person could hack into these insecure devices and literally kill someone**, so it is time that the healthcare industry started taking medical device IoT security more seriously.

#### 4. Hacking IoT medical devices can also be used for other nefarious purposes

**Ryan Fahey** (Ryan Fahey, digital marketing manager at the InfoSec Institute, an award-winning training institute that has trained thousands of technology professional for over a decade. Nd, but after 2014 and copyright 2016. “The Internet of Things in Healthcare,” *InfoSec Institute*, <http://resources.infosecinstitute.com/category/healthcare-information-security/emerging-technologies-in-healthcare/the-internet-of-things-in-healthcare/>. Accessed Nov 14 2016) ESG

But **perhaps one of the most crucial challenges in Internet of Things medical devices is their security and keeping them and the information they contain out of the hands of thieves.** Hacking is already a concern in the IoT – in 2014, one of these “smart refrigerators” was compromised and caught sending out 750,000 spam emails. The same thing could potentially happen to a smart EKG or thermometer. Rapid7, an analytics and data security firm, made a case study about IoT baby monitors and found that many of the top manufacturers have products that can potentially be exploited by hackers. In addition, we have discussed in other posts the rising menace of ransomware in healthcare. **Imagine if you will a scenario where hackers have taken control of an array of lifesaving devices and disabled them until a fee is paid. When Hollywood Presbyterian was hacked and could not access medical records, they coughed up $17,000.** Then there is the danger of all this patient data being stolen and used for nefarious purposes or sold on the black market. **Hacked medical records are already being used to create phony prescriptions or billing fraud** and the billions of Internet of Things medical devices will potentially create as many new paths of access to this information.

#### 5. Heathcare IoT can be used for discriminatory health insurance

**Scott Peppet 14** (Scott R. Peppet, Professor of Law in University of Colorado, March 1st, 2014, “Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent”, *Social Science Research Network,* [*http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=2409074*](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409074)October 10th, 2016) CDY

Sensor fusion and Big Data analysis combine to create the possibility that everything reveals everything on the Internet of Things. **Although a consumer may use a Fitbit solely for wellness-related purposes, such data could easily help an insurer draw inferences about that consumer to set premiums more accurately (e.g., amount of exercise may influence health or life insurance**, or amount and quality of sleep may influence auto insurance); aid a lender in assessing the consumer’s creditworthiness (e.g., conscientious exercisers may be better credit risks); help an employer determine whom to hire (e.g., those with healthy personal habits may turn out to be more diligent employees); or even help a retailer price discriminate (e.g., those wearing a Fitbit may have higher incomes than those without). To the extent that context-violative data use breaks privacy norms—as Helen Nissenbaum and others have argued—consumer sensors will disrupt consumers’ expectations.239 This is Big Data at an entirely new scale, brought about by the proliferation of little sensors.

#### 6. Healthcare IoT is expensive and inconvenient

**Ricardo Mousinho et al, 2016** (Ricardo Mousinho, scientist at Prescient Healthcare Group, Philip Winkworth, PhD, Associate Consultant at Prescient Healthcare Group, Roland Galgoczy, Associate Consultant at Prescient Healthcare Group, Benjamin Hope, Managing Principal at Prescient Healthcare Group. 2016. “Perspectives on IoT in healthcare in 2016,” *Prescient Healthcare Group*, <http://www.prescienthg.com/wp-content/uploads/2016/02/Perspectives-on-IoT-in-healthcare-in-2016-Part1.pdf>. Accessed Nov 14 2016. Page 2-3) ESG

Another key issue is the word “smart”. Currently, “smart” is taken to mean “expensive”, even though it could deliver costsavings through improved compliance and reductions in hospitalisation time. **To health authorities, it is very expensive for each patient to obtain access to these smart devices, and health authorities will not be able to afford to introduce these technologies** unless they are proven to be cost-effective and highly beneficial to **patients. Patients have to pay out of pocket for these devices at the moment**, unless the treatment costs are covered by private insurers or the technology is cost-effective to payers. The failure of IoT in healthcare to live up to the hype is attributed not only to the price or security issues but also to the fact that most companies are not looking at the fundamental value offering for the patient, which is that having a userfriendly “remote” that is on or with the patient at most times (i.e., a smartphone or smartwatch) allows for communication with healthcare professionals in the simplest and most efficacious way possible. **It’s also likely that very few patients would be willing to wear multiple sensors on different parts of their bodies, or to sacrifice many nights out because they have to be at home to log their daily readings into a modem-like device which stores and sends findings to physicians about daily insulin fluctuations, for example.**

### AT: Agriculture

#### 1. In the poorer parts of the world, sophisticated agricultural technologies are less important than other essentials like education

**Evan Fraser and Sylvian Charlebois 2016** (Evan Fraser, Canada research chair and professor of geography & Sylvian Charlebois, professor of food distribution and policy. “Automated farming: good news for food security, bad news for job security?,” The Guardian. <https://www.theguardian.com/sustainable-business/2016/feb/18/automated-farming-food-security-rural-jobs-unemployment-technology>) EL

Many experts are looking forward to a future where the Internet of Things (where physical objects such as vehicles, buildings and devices are connected to collect and exchange data) is applied to food and farming to create an Internet of Living Things. In this future, advanced sensors embedded in fields, waterways, irrigation systems and tractors will combine with machine-learning systems, genome-identifying devices and data dashboards to give rise to a generation of smart farming technology that will have the capacity to sense and respond to its environment in a way that maximises production while minimising negative impact. However, **there are problems. In many of the poorer parts of the world, sophisticated agricultural technologies are much less important than education, healthcare, access to capital, sound governance and basic infrastructure. For the HIV positive farmer supporting her family on just one hectare in rural Malawi, satellite driven tractors and high productivity beef germplasm are about as useful as a moondust.**

#### 2. Hunger is not caused by scarcity but by how food is used

**Eric Holt Gimenez, 2012** (Eric Holt Gimenez, executive director of Food First/Institute for Food and Development Policy. December 18th 2014. “We Already Grow Enough Food for 10 Billion People and Still Can’t End Hunger,” *The Huffington Post*, <http://www.huffingtonpost.com/eric-holt-gimenez/world-hunger_b_1463429.html>. Accessed Nov 14 2016) ESG

A new a study from McGill University and the University of Minnesota published in the journal Nature compared organic and conventional yields from 66 studies and over 300 trials. Researchers found that on average, conventional systems out-yielded organic farms by 25 percent — mostly for grains, and depending on conditions. Embracing the current conventional wisdom, the authors argue for a combination of conventional and organic farming to meet “the twin challenge of feeding a growing population, with rising demand for meat and high-calorie diets, while simultaneously minimizing its global environmental impacts.” Unfortunately, neither the study nor the conventional wisdom addresses the real cause of hunger. **Hunger is caused by poverty and inequality, not scarcity. For the past two decades, the rate of global food production has increased faster than the rate of global population growth. The world already produces more than 1 ½ times enough food to feed everyone on the planet.** That’s enough to feed 10 billion people, the population peak we expect by 2050. But the people making less than $2 a day — most of whom are resource-poor farmers cultivating unviably small plots of land — can’t afford to buy this food. **In reality, the bulk of industrially-produced grain crops goes to biofuels and confined animal feedlots rather than food for the 1 billion hungry. The call to double food production by 2050 only applies if we continue to prioritize the growing population of livestock and automobiles over hungry people.**

#### 3. Farmers don’t realize that they are losing ownership of their data to corporate servers when using sensors

Lina Khan, 2013 (Lina Khan, writer for AlterNet, an award-winning news magazine and online community to inspire action and advocacy on the environment, human rights and civil liberties, social justice, media, health care issues, and more. December 30, 2013. “Monsanto's Terrifying New Scheme: Massive Amounts of Data Collection,” *Alternet*, <http://www.alternet.org/food/monsantos-terrifying-new-scheme-massive-amounts-data-collection>. DoA: November 11, 2016.) NB

Farm advocacy groups are now scrambling to understand how — if given free rein — these corporations could misuse the data they collect. “We’re signing up for things without knowing what we’re giving up,” said Mark Nelson, director of commodities at the Kansas Farm Bureau. In May, the American Farm Bureau Federation, a national lobbying group,published a policy brief outlining some potential risks around these data-driven farm tools. For farmers, the most immediate question is who owns the information these technologies capture. Many farmers have been collecting digitized yield data on their operations since the 1990s, when high-tech farm tools first emerged. But that information would sit on a tractor or monitor until the farmer manually transferred it to his computer, or handed a USB stick to an agronomist to analyze. Now, however, smart devices can wirelessly transfer data straight to a corporation’s servers, sometimes without a farmer’s knowledge. “When I start storing information up on the Internet, I lose control of it,” said Walt Bones, who farms in Parker, S.D., and served as state agriculture secretary.

#### This is massively harmful because,

Lina Khan, 2013 (Lina Khan, writer for AlterNet, an award-winning news magazine and online community to inspire action and advocacy on the environment, human rights and civil liberties, social justice, media, health care issues, and more. December 30, 2013. “Monsanto's Terrifying New Scheme: Massive Amounts of Data Collection,” *Alternet*, <http://www.alternet.org/food/monsantos-terrifying-new-scheme-massive-amounts-data-collection>. DoA: November 11, 2016.) NB

How corporations use the information is another central concern. One worry is the giants will harness the data to engage in price discrimination, in which they charge some farmers more than others for the same product. For example, details on the economic worth of a farm operation could empower Monsanto or DuPont to calculate the exact value the farm derives from its products. Monsanto already varies its prices by region, so that Illinois farmers with a bumper crop might be charged more for seeds than Texas farmers facing a drought. Bigger heaps of data would enable these companies to price discriminate more finely, not just among different geographic regions but between neighbors.

#### 4. Data from farmers is taken by corporations and sold to market speculators

**Devare 2015** (Medha Devare, data and knowledge manager; may 2015; "Medicine, open data and the smallholder farmer"; Godan; <http://www.godan.info/responses-to-odigodan-discussion-paper-may-2015> ) AM

Some of the examples used do not give a balanced perspective of the downside of opening data. For example weather **data**, especially rainfall, **can also be used to predict food grain production and enable forecast of prices in international markets**. In the food price crises of 2007-2009, **the rise of food prices has now been attributed to stock market speculators** especially in the Middle East. **Open data on agriculture can be used against the interest of farmers and consumers for private profit by these speculators** analyzing weather data. Similarly, **doing soil analysis to “help” farmers** also **contribute**, when aggregated and mapped geographically to predict fertilizer use very concisely. This can enable increasing profit through cartelization, hoarding, creating shortages, black marketing and increased pricing for fertilizer producers and sellers as fertilizer use is seasonal and time bound for farmers. This has been seen in India. Open land holding data, again in India, led to land grabbing. Supermarkets and fast food restaurant chains collect data on food consumption patterns etc. and aggregate them with other public data to create advertisements and pricing structures to maximize their profits at the cost of and against the interests of consumers. **Several business ventures have recently started, in the guise of aiding “poor”, small farmers “free” or at “low cost” services through providing automated weather stations, soil sensors** and laboratory analysis etc.. **These ventures aggregate the data and sell the data sets for profit without any regulatory mechanisms and sharing profits with farmers whose data it legally should be. With new technologies such as sensors and the Internet of Things in machinery, tools and equipment a large volume of agricultural and nutritional data is already being collected with very little information or control of those who “own” the tools or use them. John Deere now considers its tractors and other equipment as legally “software” and not a machine. It does not sell a machine but leases, as Microsoft or Apple does, the use of its software. This as John Deere claims gives them the right to use data generated as “feedback” from their machinery**. There is a growing farmers’ movement on their rights to their data generated from their farms. The paper does not discuss this issue and how it can impact upon opening of agricultural data. The discussion paper advocates opening agricultural and nutritional data without any consideration of how to support the costs in generating, managing and enabling its effective use by countries and communities who do not have the capacities to generate, manage and use it. Opening data without enabling effective, equitable use can be considered a form of piracy. GODAN should consider these issues in formulating its advocacy. Advocacy for opening data must also include advocacy for open ICT tools and techniques such as storage, search and analytical algorithms and open technologies for agriculture and improving nutrition.

#### 5. IoT is too expensive for farmers to implement

**David Curry, 2016** (David Curry, contributing writer for *ReadWrite*. August 4th 2016. “IoT grows crops best, but still too pricy for farmers,” *ReadWrite*, <http://readwrite.com/2016/08/04/iot-agriculture-costs-it4/>. Accessed November 16th 2016) ESG

The Internet of Things (IoT) is coming to the agriculture industry, but a new report suggests that service costs and niche products are slowing adoption of the new technologies. Benefits of IoT in agriculture includes better yield rates and reductions in the amount of water, soil, and seed needed**. The worry, for farmers, is the implementation of IoT systems and cost of service surpasses the costs saved from using the technology.** It is not the first industry to be on the fence on IoT benefits. Retailers have had a wealth of IoT startups to choose from, offering data analytics on shopper behaviors, but most have skipped the services, possibly due to the service charges outweighing the added revenue per customer. In agriculture, there are a few suppliers that offer services at an annual cost. One of those is OnFarm Systems, which provides its Grower Dashboard, a platform to manage farm sensors, monitor temperature, cloud, and water irrigation, schedule tasks, and view analytics. That comes alongside SMS alerts, maps, weather data, storage and backup and a messaging service. **For a single user, the cost is $100 a year, but OnFarm limits the user to three data streams and one property, whereas the $500 a year package gives unlimited integrated data, acres, and data feeds. On top of that, an additional $100 is added for every virtual weather station the customer purchases.** Agriculture margins make tech investment tough Others mentioned in the Lux Research report don’t provide costs on their website. Semios, for example, shows five different parts of its IoT platform for orchard and soil-based farming, but doesn’t say if the five features come separate or are available in one annual package. **Phytech is even more expensive than OnFarm, costing $500 per acre.** In case studies, Phytech says it can reduce water usage by 10 percent in two weeks, but is that reduction enough to cover the costs? All depends on the produce cost and how much a farmer can fit onto an acre of land. **The agriculture industry is not seeing large profits and service providers need to be able to show their value if they want customers that send payment every year.** If 10 percent reduction in water usage or 20 percent increase in yield rate is worth it, we are bound to see more of these IoT startups enter the market, but if its not, **we might see farmers firmly reject these emerging technologies** for a few more years.

### AT: Earthquake Sensors

#### 1. Predicting exactly how an earthquake strikes is near impossible

**Eric Niiler, 2015** (Eric Niiler, reporter on science for *The Washington Post*. November 2nd 2015. “Why it is so hard to get an earthquake warning system,” *The Washington Post*, <https://www.washingtonpost.com/national/health-science/when-an-earthquake-is-coming-how-can-you-get-even-a-little-warning/2015/10/30/df12c640-63c1-11e5-9757-e49273f05f65_story.html>. Accessed Nov 13 2016) ESG

Now researchers say that with a combination of ground sensors and satellite-based instruments, they are getting closer to giving people a crucial minute or two of warning, though they acknowledge that **predicting exactly where and when an earthquake will strike remains an elusive goal.** “When I started in this field 30 years ago, that was the goal,” **Thomas Heaton, a professor of geology and geophysics at the California Institute of Technology, said** about whether it’s possible to make such predictions. “But **the answer today is pretty clearly, no. The more we looked at the problem, the more we understood that all the earthquakes aren’t the same.”**

#### 2. Seismic sensors are vulnerable to hacking

**BBC News 2016** (BBC News, operational business division of the British Broadcasting Corporation responsible for the gathering and broadcasting of news. August 7th 2016. “Security of seismic sensor grid probed,” *BBC News*, <http://www.bbc.com/news/technology-37001301>. Accessed November 13th 2016) ESG

**Thousands of seismic sensors monitoring geological activity are vulnerable to cyber attack, suggests research.** The poor security controls around the way the sensors transmit data were detailed in a presentation at the Def Con hacker convention. **Researchers found ways to fool and overload sensors so monitoring systems would get wildly inaccurate readings.** The findings have been reported to the US computer emergency organisation that oversees national infrastructure. Nanometrics, the company that makes the sensor system that was probed disputed the researchers' findings.

#### 3. Furthermore, mass alerts to citizens are currently implausible

**Eric Niiler, 2015** (Eric Niiler, reporter on science for *The Washington Post*. November 2nd 2015. “Why it is so hard to get an earthquake warning system,” *The Washington Post*, <https://www.washingtonpost.com/national/health-science/when-an-earthquake-is-coming-how-can-you-get-even-a-little-warning/2015/10/30/df12c640-63c1-11e5-9757-e49273f05f65_story.html>. Accessed Nov 13 2016) ESG

In 2013, the California legislature passed a bill requiring the establishment of such an alert system, but it didn’t approve any money. The federal government has approved only a small portion of the funds needed to build and operate the system. According to Doug Given, the USGS earthquake early-warning coordinator, about 600 of the planned 1,600 sensors have been installed, mostly paid for by cooperating companies and utilities. For Given and others, the real challenge is not so much the science but the software engineering needed to get the alert out. The trick is picking up the initial signal of the quake, called the p-wave, or primary wave, and getting out that information before the s-wave, or shock wave, hits a particular spot, a time lag that can be as little as 10 seconds or as long as several minutes, depending on the spot’s distance from the quake’s epicenter. “How do you get the notification out to millions of people in as little time as possible?” Given said from his office in Pasadena, Calif. “**Most people assume that you can just send them a text message. No system can send 12 million text messages at one time.” (The population of the Los Angeles area is more than 18 million.) Until such issues are worked out, earthquake alerts are currently going out only to first responders, utilities and companies that have earthquake-sensitive operations**, Given said. The ShakeAlert system was used during an August 2014 earthquake that struck Napa Valley, just northeast of San Francisco. The Bay Area Rapid Transit system received the alert, however because the temblor hit at 3:20 a.m. trains weren’t running. **Sending mass alerts to “the general public is the very last step,”** Given said. “It will require a significant amount of training and education. With the first Amber Alerts, many people were annoyed, and very upset. There’s a lot of social science and psychology to have alerts go right with the public.”

### AT: Vaccines

#### 1. For vaccines to be effective, people need to be able to have access – to the extent that many developing countries lack infrastructure. Nazmus Sakib Miazi gives at least THREE ways this might be true.

#### First, cost.

**Nazmus Sakib Miazi et al 2015** (Nazmus Sakib Miazi, Graduate Research Assistant, Software and Information Systems, University of North Carolina, Zenville Erasmus for the Dept of Computer Science at the University of the Western Cape, Abdur Razzaque for the Wireless Laboratory at the International Center for Theoretical Physics, Marco Zennaro for Wireless Laboratory at the International Center for Theoretical Physics, and Antoine Bagula for the Dept of Computer Science at the University of the Western Cape. 2015. “Enabling the Internet of Things in Developing Countries: Opportunities and Challenges,” *International Center for Theoretical Physics,* <http://wireless.ictp.it/Papers/IoT_Developing.pdf>. Accessed Nov 19 2016) ESG

The IoT provides a great opportunity for developing countries to leapfrog from poorly prepared to scientifically and technologically equipped countries which can use the IoT technology to face their current and future challenges by tap- ping into the potential provided by this technology. However, such opportunity may become reality only if the developing world is ready to embark into this technology at the same pace as scientists and technologists of the developed world and financial challenges related to these technologies are addressed. These include low cost of acquisition, maintenance and financial sustainability. As currently perceived, sensor devices are the raw material of the IoT. **Such devices are still expensive for many countries of the developing world when accounting for the cost of acquisition and shipping from the manufacturing companies which are mainly located in the developed countries. This may hamper their wide and ubiquitous deployment in the developing world. Furthermore, for such devices, cost and field-readiness are still closely related** while the most field ready devices are usually proprietary devices with vendor- locked software, sometimes updated frequently at recurrent fees or cost. **This leads to higher cost of maintenance and operation which also leads to a challenging financial sustainability situation for those operating IoT businesses.** Many of these challenges may be addressed through local IoT expertise, the use of open source hardware and software, and strong collaboration between scientists and technologists of the developed and developing world. Such collaboration will enable the IoT4D dream to become reality.

#### Second, internet access.

**Nazmus Sakib Miazi et al 2015** (Nazmus Sakib Miazi, Graduate Research Assistant, Software and Information Systems, University of North Carolina, Zenville Erasmus for the Dept of Computer Science at the University of the Western Cape, Abdur Razzaque for the Wireless Laboratory at the International Center for Theoretical Physics, Marco Zennaro for Wireless Laboratory at the International Center for Theoretical Physics, and Antoine Bagula for the Dept of Computer Science at the University of the Western Cape. 2015. “Enabling the Internet of Things in Developing Countries: Opportunities and Challenges,” *International Center for Theoretical Physics,* <http://wireless.ictp.it/Papers/IoT_Developing.pdf>. Accessed Nov 19 2016) ESG

1) Internet Connectivity: Internet Connectivity is a prime issue, when we want to enable IoT. Internet of Things demands flawless and adequate connectivity among every particular thing. To sustain flawless connectivity, **it needs fast internet speed, a continuous power supply, robust backup systems and reliable and scalable infrastructure. Facilitating the end users with high speed internet in developing countries is a huge challenge. To deploy wired backbone throughout the whole country is formidably costly, and it is kind of impossible for them to develop a countrywide wired network to facilitate every end-user.** An easy alternative is to provide internet access through wireless technologies, like 3G, WiMAX, 4G-LTE, etc. This invokes other kinds of problems concerning lower internet speed, high power consumption, high cost per unit usage ratio, etc. So, the authorities can deploy a hybrid model of internet backbone over the whole country, consisting of a fiber-optic national data-highway, local and national data centers, regional WiMAX and 4G service points, etc. The main challenge here is to deploy a hybrid backbone over the country, that trades-off with the problems and facilitates the end-users with optimal utility, that can be sufficient to enable IoT in these countries.

#### Third, energy usage.

**Nazmus Sakib Miazi et al 2015** (Nazmus Sakib Miazi, Graduate Research Assistant, Software and Information Systems, University of North Carolina, Zenville Erasmus for the Dept of Computer Science at the University of the Western Cape, Abdur Razzaque for the Wireless Laboratory at the International Center for Theoretical Physics, Marco Zennaro for Wireless Laboratory at the International Center for Theoretical Physics, and Antoine Bagula for the Dept of Computer Science at the University of the Western Cape. 2015. “Enabling the Internet of Things in Developing Countries: Opportunities and Challenges,” *International Center for Theoretical Physics,* <http://wireless.ictp.it/Papers/IoT_Developing.pdf>. Accessed Nov 19 2016) ESG

3) Power Resources: **Compared to developed countries, the planning of electricity for developing countries presents itself as a complicated dilemma. The challenge surpasses the mere acquisition of financing for energy related investments. Energy development is challenging as electric power industries are among the most intensive in an economy.** **This leads to the severe draining of financial resources.** IoT for developing countries (IoT4D) will aid in provid- ing power solutions by enabling clean energy technologies, creating smarter energy markets and by optimizing the imple- mentation of existing products. For example, to improve the use of energy in homes, the IoT will automate and promote energy efficient practices such as the running of appliances at off-peak times. In terms of a solution presented by IoT, servicing customers with information regarding utilities, devices known as smart meters can provide real-time, two-way communication be- tween customers and devices in their perusal. Benefits involve granular detail to customers about their electricity usage. Smart meters also aid customers in modifying their energy consumption in relation to current prices. A smart meter also allows the collection of data automatically. This negates the need for a company needing to send out an engineer to manually collect data readings from such a meter. It also serves as an effective means to detect outages and the necessity of repairs [11].

#### 2. The problem is that vaccines are too expensive, even doctors without borders cites this as the main problem

James Maynard 2015 (James Maynard is an author and writer for Tech Times. January 22, 2016. “Vaccine Costs in Developing Countries Too High, Many Blame GSK, Pfizer,” Tech Times. <http://www.techtimes.com/articles/28166/20150122/vaccine-costs-developing-countries-high-many-blame-gsk-pfizer.htm> DOA: 11/20/16) CDY

**Vaccine costs in developing countries are too high to provide adequate attention to at-risk populations,** and some healthcare professionals are blaming pharmaceutical companies such as Pfizer and GlaxoSmithKline (GSK) for high prices. **Doctors Without Borders is calling** on GlaxoSmithKline and Pfizer **to reduce prices for vital vaccines, in an effort to provide protection to residents in poorer countries.** The volunteer group has determined that vaccine prices need to reach five dollars per immunization to provide adequate coverage. The Right Shot: Bringing Down Barriers to Affordable and Adapted Vaccines, a report detailing the financial costs of immunizations, reveals the price of inoculations is currently dozens of times more expensive than it was in 2001. "**The price to fully vaccinate a child is 68 times more expensive than it was just over a decade ago, mainly because a handful of big pharmaceutical companies are overcharging donors and developing countries for vaccines that already earn them billions of dollars in wealthy countries**," Rohit Malpani, director of policy and analysis for Doctors Without Borders, [said](http://www.doctorswithoutborders.org/article/msf-calls-gsk-and-pfizer-slash-pneumo-vaccine-price-5-child-poor-countries" \t "_blank).

#### Between the expense of vaccines *and* the internet of things, it is unlikely this is the solution

#### 3. There is no panacea for vaccination: a myriad of factors must be solved

**World Health Organization** (World Health Organization, UNICEF, and The World Bank. “State of the World’s Vaccines and Immunization: Challenges to Sustaining Progress,” World Health Organization, UNICEF, and The World Bank. <http://www.portal.pmnch.org/immunization/fact_sheet_challenges.pdf>) EL

Despite extraordinary progress in immunizing more children over the past decade, in 2007, 24 million children—almost 20 percent of the children born each year—did not get the complete routine immunizations scheduled for their first year of life. **Most of these 24 million unimmunized or incompletely-immunized children live in the poorest countries, where many factors combine to thwart attempts to raise vaccine coverage rates—fragile or non-existent health service infrastructure, difficult geographical terrain and armed conflict, to mention just three.**

#### 4. Vaccination rates are positive and growing

**Angela Shen et al. 2014** (Angela Shen et al, December 2014, Senior Science Policy Advisor at the National Vaccine Program Office, *NCBI*, " The future of routine immunization in the developing world: challenges and opportunities", https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4307855/, Accessed 11/07/2016) SEO

**Global coverage for the third dose of the diphtheria, tetanus, and pertussis vaccine (DTP3) increased from 73% in 2000 to 82% in 2008** but has remained stalled since then, hovering around 83%.[28](http://www.ghspjournal.org/content/2/4/381.full#ref-28) Within-country variations are substantial, even in countries with high nationwide coverage.[29](http://www.ghspjournal.org/content/2/4/381.full#ref-29) Data from the Demographic and Health Surveys from several African countries show that coverage is consistently lower in the poorest wealth quintile than in the highest quintile ([Figure 2](http://www.ghspjournal.org/content/2/4/381.full#F2)). The children who are missed tend to be those most in need of the protection that immunization confers. In many LLMICs, immunization budgets are currently insufficient to sustain programs and incorporate the new, costlier vaccines, although there is fiscal space to absorb costs.[50](http://www.ghspjournal.org/content/2/4/381.full#ref-50) New vaccines have added both tremendous benefit and costs to the original EPI blueprint.[7](http://www.ghspjournal.org/content/2/4/381.full#ref-7) For example, the Gavi/UNICEF cost of the human papillomavirus (HPV) vaccine to protect girls against cervical cancer is about US$4.50 per dose, with 3 doses recommended (total cost $13.50). In 2001, the total cost of the original set of 6 WHO-recommended vaccines was under US$1 ([Figure 3](http://www.ghspjournal.org/content/2/4/381.full#F3)). With the introduction of a combination 5-in-1 pentavalent vaccine in 2005, children became protected against 2 additional vaccine-preventable diseases, and the total vaccine costs increased to about $11. In 2014, the total cost of 11 WHO-recommended vaccines reached approximately $21, with an additional $13.50 to vaccinate girls against HPV. Looking forward, adding an inactivated polio vaccine (IPV) to support the polio eradication efforts will add $1.26 to the schedule, bringing the total vaccine costs to about $23 for boys through age 18 and to $36 for girls. Note that prices vary by brand of vaccine and vaccine presentation (eg, multi-dose vials, liquid formulation). Delivery costs, estimated by Lydon and colleagues (2014), add about $25 per child, bringing the total delivery costs to fully immunize a child to around $50 to $60.[7](http://www.ghspjournal.org/content/2/4/381.full#ref-7),[51](http://www.ghspjournal.org/content/2/4/381.full#ref-51) These delivery costs are most likely underestimates.

#### 5. This “smart fridge” is yet to be deployed – they are more speculative than they let on

**Barb Edson 2016** (General Manager, Marketing, Cloud and Enterprise for Microsoft. August 16, 2016. “IoT-enabled Smart Fridge helps manage vaccines and saves lives,” Microsoft. <https://blogs.microsoft.com/iot/2016/08/16/iot-enabled-smart-fridge-helps-manage-vaccines-and-saves-lives/> DOA: 11/20/16) CDY

Controlled refrigeration and monitoring also helps reduce financial losses. “Physicians generally have $40,000 to $60,000 worth of vaccines in their refrigerators,” says Lowenstein. “If the clinic suffers a power outage or the traditional fridge fails, they risk losing the entire inventory of vaccines.” By using automated processes to manage inventory through IoT sensors, the Fridge can deliver proactive alerts on inventory shortages or changes in temperature. In addition, Weka estimates that a medical practice that dispenses approximately 400 vaccines per month could reduce human-resource costs by more than $1,000 a month with the Fridge’s monitoring system. This system helps ensure that the first vaccines in the refrigerator are the first that come out, so patients never receive an expired or recalled vaccine, and it reduces the manual task of vaccine management by clinicians. The Smart Fridge is a great example of how companies can accelerate digital transformation with smart solutions to increase staff efficiency and quality control and automate inventory management. **Weka’s Smart Fridge is currently scheduled to go to market at the beginning of 2017.** Read more about how the [Weka Smart Fridge](https://customers.microsoft.com/Pages/CustomerStory.aspx?recid=28426) is improving vaccine management. And to learn more about how Microsoft IoT can transform your business, visit [www.InternetofYourThings.com](http://www.internetofyourthings.com/).

### AT: Water Saved

#### 1. There is no panacea to water conservation – IoT alone can’t solve

Rinkesh 2016 (Rinkesh, writes on various environmental and renewable energy related topics. 2016 “What is Water Scarcity?” from Conserve Energy future. <http://www.conserve-energy-future.com/causes-effects-solutions-of-water-scarcity.php> DOA: 11/5/16 ) ESM

Solutions for Water Scarcity Education: There are plenty of opportunities out there that people can use in order to learn more about the world around them. By educating those who are not dealing with water scarcity, they can be in a position to help. Those who are dealing with it can get educated on how they can prevent the problem from becoming even worse in the future. Recycle Water: There are plenty of technologies out there that allow you to [recycle rainwater](http://www.conserve-energy-future.com/Advantages_Disadvantages_Rainwater_Harvesting.php" \t "_blank) and other water that you may be using in your home. Consider learning about how you can recycle water. Not only does it help to prevent scarcity, but it can save you some money as well. Advance Technology Related to Water Conservation: There has been a lot of work in the world of water conservation, but there is also a lot that needs to be done in order to ensure that the rest of the world is able to [conserve water](http://www.conserve-energy-future.com/various-ways-to-conserve-water.php" \t "_blank). Putting money and effort into conservation could be life saving. Improve Practices Related to Farming: Farming and irrigation are often a huge culprit when it comes to water scarcity. Because of that, we need to improve practices so that we don’t use as much water and those who are using water are using it to its fullest potential. Technology also needs to advance in this manner. Improve Sewage Systems: Clean drinking water starts with a good sewage system. Without proper sanitation, the water in an area becomes ridden with disease and any number of other problems. By improving the sewage systems in these areas, we can prevent water scarcity from becoming any worse. Support Clean Water Initiatives: There are organizations located all over the world that are looking to bring clean water to areas that don’t have it. Consider donating to these organizations, either with your time, your skills, or your finances (whichever you can afford to give to them**).** So, as you can see, there are a lot of things that we need to consider when we’re looking at water scarcity and how we can deal with it. If we start to look at this issue as a whole, and we work hard to make sure that we are able to make a difference when it comes to this widespread issue, we’re going to be in a much better place to help people all over the world in preventing this issue from getting worse.

#### 2. E-waste from the Internet of Things could pollute water sources

**Anand Sankar, 2014** (Anand Sankar, software architect and coder. November 10th 2014. “Internet of Things: The Good, the Bad, and the Ugly,” *Anand Mani Sankar*, <http://anandmanisankar.com/posts/IoT-internet-of-things-good-bad-ugly/>. Accessed 11/18/16) ESG

The possible explosion of e-waste is another growing concern. The rapid mushrooming of small electronic devices could significantly contribute to the already growing e-waste. **A concern regarding IoT technologies pertains to the environmental impacts of the manufacture, use, and eventual disposal of all these semiconductor-rich devices.** Modern electronics are replete with a wide variety of heavy metals and rare-earth metals, as well as highly toxic synthetic chemicals. This makes them extremely difficult to properly recycle. **Electronic components are often simply incinerated or dumped in regular landfills, thereby polluting soil, groundwater, surface water, and air.**

#### 3. Cheap, easy water sensors are infeasible

**Josh Howgego, 2015** (Josh Howgego, Science journalist/writer/editor at New Scientist magazine. May 11th 2015. “The impossible water sensor,” *Education In Chemistry,* <http://www.rsc.org/eic/2015/05/water-sensors-pollution>.Accessed 11/19/2016) ESG

Ultimately though, if Dermot is to create a sensor design that can be deployed in its millions across Europe, merely revising the Oberstown design won’t be enough. **To make sensing easy and cheap, sensors should work autonomously for long periods, ideally several years. With this sensor, that isn’t possible for three reasons. Firstly, the reagents are only stable for about a year**, after which time they begin to chemically degrade and the reaction stoichiometry skews. **Secondly, the sensor needs regular calibration**. That means making sure the measured light absorbance really does correspond to a correct phosphate concentration by injecting standard solutions with known amounts of phosphate in them and using these to compensate for any discrepancies. **Thirdly, the sensor is in sewage, a harsh environment.** Lots of bugs live in raw sewage and it is not long before these begin to multiply and create a bio-gunge that blocks the sensor’s microfluidics. Dermot says all these factors mean **a sensor can run for no more than about three months before it needs attention from a scientist.** ‘Three months service is good,’ says Dermot, ‘but it needs to be extended further to drive down the cost’.

#### 4. **The biggest issue for the implemetation smart water meters is cost**

Ucilia Wang, 2015. (Ucilia Wang, Writer for the *Wall Street Journal*. 5/5/2015. “Water meters begin to get smarter,” *The Wall Street Journal*, http://www.wsj.com/articles/water-meters-begin-to-get-smarter-1430881505. DOA: 11/19/16.) TG

**Expense is the biggest obstacle to broader adoption of smart meters. Each connected meter can cost as much as $300. Running a full smart meter network can also be expensive**, depending on features built into the meters, how frequently data is collected and how much analysis the utility performs. While utilities get some savings from eliminating meter readers, the **smart meters are more expensive to repair and maintain than traditional meters—for instance, they have batteries that need to be replaced more often because the meters are frequently collecting and transmitting data.**

### AT: Bitcoins Good

#### 1. Bitcoins can exist with out IoT, therefore, the argument is non-unique. Bitcoins are simply a digital currency, they have noting to do with the IoT.

#### 2. **Bitcoins are self regulated, which means that your money is completely unprotected**

Couts 2013 ([Andrew Couts](http://www.digitaltrends.com/users/andrew_couts/), covers a wide swath of consumer technology topics, with particular focus on the intersection of technology, law, politics, and policy. December 7, 2013 “WHY NOBODY IN THEIR RIGHT MIND SHOULD GET INTO BITCOIN RIGHT NOW” from Digital Trends. <http://www.digitaltrends.com/opinion/nobody-right-mind-get-bitcoin-right-now/> DOA: 11/3/16) ESM

Right now, Bitcoin is completely self-regulated. There’s a whole complicated system in place to keep the currency on the level. Problem is, that’s where the oversight stops. As [The New York Times reported](http://dealbook.nytimes.com/2013/12/05/in-the-murky-world-of-bitcoin-fraud-is-quicker-than-the-law/?_r=0" \t "_blank) on Friday, the reason financial regulators haven’t put their stamp on Bitcoin yet is because “government authorities do not agree on which laws apply to Bitcoin — or even on what Bitcoin is.” That’s right – governments can’t even decide what Bitcoin is. That fact alone should send any responsible investor running for a bunker. (High-risk investors, however, likely see the lack of government intervention as Bitcoin’s most valuable feature.) What the Bitcoin free-for-all means in practice is that your Bitcoin stash is roughly as protected as a nudist beekeeper. Unlike your bank account, the federal government offers no guarantees that your Bitcoin wallet is safe. And if someone steals your Bitcoins, the police are probably not going to do a damn thing about it. Again, as the Times reports, “…for crimes contained within the Bitcoin network – like thefts from apparently reputable online wallets where Bitcoins are stored – there has been almost no accountability.”

#### **3. Bitcoins aren’t necessary unless you’re buying something illegal**

Couts 2013 ([Andrew Couts](http://www.digitaltrends.com/users/andrew_couts/), covers a wide swath of consumer technology topics, with particular focus on the intersection of technology, law, politics, and policy. December 7, 2013 “WHY NOBODY IN THEIR RIGHT MIND SHOULD GET INTO BITCOIN RIGHT NOW” from Digital Trends. <http://www.digitaltrends.com/opinion/nobody-right-mind-get-bitcoin-right-now/> DOA: 11/3/16) ESM

As for using Bitcoin as actual money, that’s a bad idea too. First of all, it just isn’t practical. You can buy [all types of stuff](http://usebitcoins.info/" \t "_blank) using Bitcoin, but unless you want to buy something illegal, there isn’t a need to use Bitcoin at all. It’s just a novelty. But it’s worse than that. Because the price of Bitcoin changes by the day – [often drastically](http://bitcoincharts.com/charts/mtgoxUSD" \l "rg60ztgSzm1g10zm2g25zv" \t "_blank) – you could end up paying far more for [that car](http://www.digitaltrends.com/cars/buying-digital-car-digital-money-tesla-s-bought-bitcoins/) than you would have using dollars. At the end of the day, Bitcoin is a technologically and philosophically excellent idea – one that people are willing to pay real money to have a part in. It’s cool. It’s irreverent. And it is making some people [very, very rich](http://bitcoinrichlist.com/top100" \t "_blank). The price of a Bitcoin is at an all-time high right now – and it could quite possibly jump ten or a hundred times higher, making this anti-Bitcoin screed seem ridiculous. Even if that happens, however, I won’t feel an ounce of regret for recommending that everyday people keep their life savings out of Bitcoin; its value could just as easily – perhaps more easily – drop to $100, or $1, or lower. And even if it doesn’t, some A-hole hacker could swipe your entire Bitcoin fortune and walk away without a care in the world. There may come a day when plunking your dollars into Bitcoin makes sense. But now is not that time.

#### 4. **Bitcoin value is unregulated and can’t be anonymous for it to function**

Knibbs 2015 ([Kate Knibbs](http://kinja.com/knibbs), staff writer, 2015 “[Bill Gates: Digital Currency Can Help the Poor, But Not Bitcoin](http://gizmodo.com/bill-gates-digital-currency-can-help-the-poor-but-not-1682346647)” from GizModo. <http://gizmodo.com/bill-gates-digital-currency-can-help-the-poor-but-not-1682346647> DOA: 11/3/16) ESM

So why not Bitcoin? The billionaire philanthropist and [redditor](http://gizmodo.com/5983465/bill-gates-shows-off-sense-of-humor-seductive-pose-in-reddit-ama) called it "an exciting new technology" in today's AMA, but he doesn't think it's a very good tool to make banking easier in emerging markets because it's so volatile and because it's anonymous: We don't use bitcoin specifically for two reasons. One is that the poor shouldn't have a currency whose value goes up and down a lot compared to their local currency. Second is that if a mistake is made in who you pay then you need to be able to reverse it so anonymity wouldn't work. Bitcoin has been touted as [a potentially revolutionary banking tool](http://www.economist.com/blogs/baobab/2014/06/cash-transfers-africa" \t "_blank) for the poor, and it's likely Gates' remarks will rankle the community. But he did offer an alternative, highlighting the uses of local digital currency like Kenya's M-Pesa over anonymous cryptocurrencies: The foundation is involved in digital money but unlike Bitcoin it would not be anonymous digital money. In Kenya M-pesa is being used for almost half of all transactions. Digital money has low transaction costs which is great for the poor because they need to do financial transactions with small amounts of money. Over the next 5 years I think digital money will catch on in India and parts of Africa and help the poorest a lot.

### AT: Education Station

#### 1. Billions of people don’t even have WiFi – they aren’t about to have an educational revolution

**Robert Bell, 2016** (Robert Bell, Executive Director of the Society of Satellite Professionals International. 2016. “Schools Go Online in the Unconnected World,” *Spacewatch Middle East*, <http://spacewatchme.com/2016/11/schools-go-online-in-the-unconnected-world/>. Accessed November 20th 2016) ESG

But two-third of public schools in Mexico still lack Internet access, and many of Puebla’s rural schools are among them. Fortunately, a Mexican nonprofit, Entrepreneurs for Technology in Education (UNETE), is doing something about it. For a Puebla school, UNETE provided computers and a Wi-Fi network, and Newcom contributed the satellite connectivity and systems that put 90 students and teachers online for the first time. Over the past 16 years, UNETE has made is possible for 2.3 million students to access modern technology in Mexican schools, and the two organizations hope to duplicate the Puebla model at hundreds of schools throughout rural Mexico. There are an estimated 3 billion Internet users in the Connected World. Another 6 billion additional devices now connect to the Web, forming the leading edge of the fast-growing Internet of Things that Ericsson predicts will total 26 billion by 2020. **More than 4 billion people, however, still live in the Unconnected World.** Thanks to satellite, the next generation living there will have greater opportunities than any generation that came before them.

## NEG EXTENSIONS

### EXT: Too Damn High

#### 1. The cost of IoT is too high for it to be widely implemented

**Tim Brugger, 2016** (Tim Brugger, freelance writer at Quality Content LLC and *Business Insider*. February 4th 2016. “Consumers aren’t ready for an Internet of Things world,” *Business Insider*, <http://www.businessinsider.com/internet-of-things-world-may-be-too-pricy-2016-2?pundits_only=0&get_all_comments=1&no_reply_filter=1>. Accessed Nov 15 2016) ESG

With so much discussion surrounding the IoT, it's not surprising that folks around the globe recognize the impact it will eventually have on our day-to-day lives. But from a consumer's perspective, understanding the upside of smart homes, cars, and cities is one thing — actually purchasing and implementing IoT devices is another matter. **The No. 1 roadblock to consumers purchasing an IoT device today is price. As often happens when new technologies are introduced to the masses, the initial costs are prohibitive for most people. According to the Accenture data, in a worldwide survey of Internet users, 62% said IoT "things" were too expensive** with Alphabet's Nest smart home hub as just one example. Smart home devices — along with smart cars — are expected to be the entrée for the general public into the realm of IoT, which is great news for Alphabet and its IoT home-technology division, Nest. But **the asking price of around $200 for a smart thermostat or WiFi home-security camera is more than most consumers are willing to shell out.**

#### 2. As of yet, the IoT is too expensive for the developing world

**Nazmus Sakib Miazi et al 2015** (Nazmus Sakib Miazi, Graduate Research Assistant, Software and Information Systems, University of North Carolina, Zenville Erasmus for the Dept of Computer Science at the University of the Western Cape, Abdur Razzaque for the Wireless Laboratory at the International Center for Theoretical Physics, Marco Zennaro for Wireless Laboratory at the International Center for Theoretical Physics, and Antoine Bagula for the Dept of Computer Science at the University of the Western Cape. 2015. “Enabling the Internet of Things in Developing Countries: Opportunities and Challenges,” *International Center for Theoretical Physics,* <http://wireless.ictp.it/Papers/IoT_Developing.pdf>. Accessed Nov 19 2016) ESG

The IoT provides a great opportunity for developing countries to leapfrog from poorly prepared to scientifically and technologically equipped countries which can use the IoT technology to face their current and future challenges by tap- ping into the potential provided by this technology. However, such opportunity may become reality only if the developing world is ready to embark into this technology at the same pace as scientists and technologists of the developed world and financial challenges related to these technologies are addressed. These include low cost of acquisition, maintenance and financial sustainability. As currently perceived, sensor devices are the raw material of the IoT. **Such devices are still expensive for many countries of the developing world when accounting for the cost of acquisition and shipping from the manufacturing companies which are mainly located in the developed countries. This may hamper their wide and ubiquitous deployment in the developing world. Furthermore, for such devices, cost and field-readiness are still closely related** while the most field ready devices are usually proprietary devices with vendor- locked software, sometimes updated frequently at recurrent fees or cost. **This leads to higher cost of maintenance and operation which also leads to a challenging financial sustainability situation for those operating IoT businesses.** Many of these challenges may be addressed through local IoT expertise, the use of open source hardware and software, and strong collaboration between scientists and technologists of the developed and developing world. Such collaboration will enable the IoT4D dream to become reality.

### EXT: Hacking Sucks

#### **Hospital went ☹**

Martin 2016 (Alexander Martin, staff reporter at the register. Oct. 31 2016. Appointments on hold as (computer) virus wreaks havoc with NHS trust systems, *The Register*, <http://www.theregister.co.uk/2016/10/31/virus_shuts_down_nhs_trust/>. Accessed on 11/20/16) DIB

An NHS trust in England shut down all of its IT systems today and has all but ground to a halt in general after a virus compromised them on Sunday. In a bright-red warning labelled "Major incident" on the website for Northern Lincolnshire & Goole NHS Foundation Trust, patients are warned that their appointments have been cancelled due to a virus infecting electronic systems. The trust announced that it has "taken the decision, following expert advice, to shut down the majority of our systems so we can isolate and destroy it". A major incident has been called and all planned operations, outpatient appointments and diagnostic procedures have been cancelled for today and tomorrow. All adult patients (over 18) should presume their appointment/procedure has been cancelled unless they are contacted. Those who turn up will be turned away.

#### Cybercrime is increasing, will cost 6 trillion by 2021, and targets national security

Vig 2016 (Tarun Vig, Co-founder of Innefu Labs. 11/7/2016. “How Artificial Intelligence Can be Used to Combat Increasing Cyber Attacks,”*BusinessWorld*, http://businessworld.in/article/How-Artificial-Intelligence-Can-Be-Used-To-Combat-Increasing-Cyber-Attacks/07-11-2016-107865/. DOA: 11/20/16. ) TG

One of the most popular acronyms of the decade - IoT actually stands for Internet of Things but due to the rising cyber crime cases in the past few years, many are decoding it as Internet of Threats. Cybersecurity Ventures, a pioneer organisation in the field of internet security, claims that **cyber crime is going to increase the world expenses up to 6 trillion USD annually by 2021. Today, hackers are not only targeting the corporate data, but they are also threats to the security of various countries. Recently, they managed to steal the details of a deal between the Indian Navy and French submarine maker 'DCNS' even before the deployment of Scorpène submarines.**

### EXT: NOTHING IS SECURE

#### Everything is hackable

**Rodger A. Grimes 2011** (A frequent industry speaker and educator, Roger currently works for Microsoft as a principal security architect. May 10, 2011. “Everything is hackable -- and cyber criminals can't be tracked,” InfoWorld. <http://www.infoworld.com/article/2621721/cyber-crime/everything-is-hackable----and-cyber-criminals-can-t-be-tracked.html> DOA: 11/18/16) CDY

The fact is cyber crime isn't going away anytime soon for two key reasons: First, **everything is hackable. Second and more significant: Cyber criminals rarely get caught or punished for their act. As long as committing cyber crimes remains easy and lucrative, and there's no accountability, it's not going away**. Point-and-hack simplicity Breaking into almost any company is nearly as simple as closing your eyes, pointing your finger, and saying, "Go!" In the nine years I was hired to break into organization's IT systems (always with the permission of the owner), I gained entry to every company, every hospital, every bank, every financial website, and every three-letter government agency in an hour or less -- with one exception. One company, which I had previously compromised in an hour or less, had followed my previous report's guidance. The second time around, it took me three hours to break (via a blank SQL sa password, no less).

### EXT: Authoritarianism is Bad…

#### 1. Open democracies are key to the global economy

Morton Halperin 2004

Morton Halperin et al, Senior Vice President of the Center for American Progress and Director of the Open Society Policy Center, 2005, The Democracy Advantage, p. 12

What explains the consistently superior development outcomes of democ­racies? We outline the conceptual underpinnings of democracy’s superior developmental performance in Chapter 2. The reasons are many and var­ied, but boil down to three core characteristics of representative govern­ment: shared power, openness, and adaptability. Although holding free elections is what commonly defines democracy, what makes it work is the way it disperses power. Consequently, in contrast to most autocratic governments, a broader range of interests are considered on a more regular basis. This increases the likelihood that the priorities of the general public will be weighed. Indeed, the argument that authoritarian governments can ignore special interest groups and therefore make deci­sions that are for the overall good of the society is based on a series of highly dubious assumptions. One is that the unelected leaders in these systems ac­tually have the interest of the public at heart. The behavior of Fidel Castro in Cuba, Kim Jung-Il in North Korea, Alexander Lukashenko in Belarus, and Hassan Ahmad al-Bashir in Sudan, to say nothing of former Iraqi dic­tator, Saddam Hussein, would strongly suggest otherwise. Another assumption is that authoritarian governments don’t have to satisfy their own special-interest constituencies. In fact, most authoritarian systems are built on the foundations of extensive patronage networks upon which they rely to stay in power. Although typically shielded from public view, these networks have enormous impacts on economic opportunity and development. The separation of powers inherent in a democracy acts as a constant reminder to the public that the central government’s powers are limited. Thus, it encourages the expansion—and the independence—of the private sector. This, in turn, fosters a climate of innovation and entre­preneurship, the engines of economic growth. The multiplicity of influences on the decision-making process in democracies also leads to more moderate and nuanced policies. This mod­erating influence contributes to one of the most distinctive qualities of democratic development—its steadiness. The ups and downs of economic growth in low-income countries are smaller in democracies. Rather than experiencing alternating bouts of boom and bust, economies in democra­cies are more likely to undergo a stable pattern of moderate gains and small declines. For poor democracies, that quality of steadiness is exceedingly important, for it means that they are more able than countries run by dic­tators to avoid economic and humanitarian catastrophes. For broad seg­ments of their populations, this is the difference between life and death. Consider this remarkable statistic: 95 percent of the worst economic performances over the past 40 years were overseen by nondemocratic gov­ernments. Similarly, virtually all contemporary refugee crises have been wrought by autocratic governments. Although shared decision-making is frequently slower, this process is more likely to weigh risks, thereby avoid­ing calamitous policies. When something is going wrong, leaders hear about it and are forced to take action.

#### 2. Democratic peace theory is sound—the preponderance of studies and the decline of conflict in the 90s proves

Halperin 5

Morton Halperin et al, Senior Vice President of the Center for American Progress and Director of the Open Society Policy Center, 2005, The Democracy Advantage, p. 12

Counter to the expectations of the prevailing school, a great deal of re­search in the 1990s on the political dimension of conflict has revealed a powerful pattern of a “democratic peace.” Democracies rarely, if ever, go to war with each other. This pattern has held from the establishment of the first modern democracies in the nineteenth century to the present. As an ever-greater share of the world’s states become democratic, the implica­tions for global peace are profound. Indeed, as the number of democracies has been increasing, major conflicts around the world (including civil wars) have declined sharply. Since 1992, they have fallen by two-thirds, numbering just 13 as of 2003.

#### 3. Environment – cross apply Li and Reuvney

#### 4. Autocracies kill at immense levels. Rj Rummel in 2002… they have killed 4x the number of their own citizens than killed in all intl and domestic wars