## AFF BLOCKS

### AT: Automation Takes Jobs

#### 1. Automation *increases* job growth – people are needed to fill new technical skills

**Mynul Khan, 2016** (Mynul Khan, CEO of Field Nation, a worldwide technology service. May 13th 2016. “Robots won’t just take jobs, they’ll create them,” *TechCrunch*, <https://techcrunch.com/2016/05/13/robots-wont-just-take-jobs-theyll-create-them/>. Accessed 10/28/2016) ESG

**Technology has not only created departments and jobs within companies, but created the need for entirely new companies and businesses. The demand for technical skills will only increase with an increase in automation**: Someone needs to fix the robot when a part is faulty. Driverless cars will still require mechanics. New jobs will be created in science, technology, engineering and mathematics (STEM) fields like nanotechnology and robotics. **A 2011 study found that one million industrial robots directly created nearly three million jobs. Of the six countries examined in the study, five saw their unemployment rates go down as the number of robots used went up**. This study showed job creation will extend beyond the STEM fields. **The authors identified six industries where employment was likely to increase directly because of robots: automotive, electronics, renewable energy, skilled systems, robotics and food and beverage.** Not everyone will need to be an engineer to find jobs created by robots. We do not need to become modern Luddites, afraid of losing our work and place in society to robots. Rather, we can welcome them, knowing they will make our lives easier, as technology always does, and knowing that by their very existence, they will create new jobs. I am looking forward to a future where robots stimulate job growth and create exciting work we can’t even imagine today.

#### 2. Furthermore, downstream employment from automation creates millions of jobs

**Peter Gorle and Andrew Clive 2011** (Peter Gorle, managing director at Metra Martech Ltd, an int’l consultancy for market research, and Andrew Clive, senior consultant at Metra Martech Ltd. February 21st 2011. “Positive Impact of Industrial Robots on Employment,” *Metra Martech*, <http://www.ifr.org/uploads/media/Metra_Martech_Study_on_robots_02.pdf>. Accessed 10/28/2016. Page 3) ESG

1.3 Employment indirectly due to the use of robotics **A much larger source of employment, at least partly due to robotics, is the newly created downstream activity necessary to support manufacturing which can only be done by robots. We have been conservative in what we have chosen to include here.** Some of the people we have spoken to, for example, would have liked us to have included large parts of the automotive sector sales and distribution employment. Our conclusion was that much of this infrastructure was in place before robots were widely used, and so not resulting from the use of robots. The best example is the communication and leisure equipment business, from distribution to retailing. In the USA, this part of retailing is of the order of 1 million. **In world terms this accounts for 3 to 5 million of jobs which would not exist if automation and robotics had not been developed to allow production of millions of electronic products, from Phones to Playstations.**

#### 3. Automation will *create* higher-level jobs by freeing up labor positions

**John Tamny, 2015** (John Tamny, a Senior Fellow in Economics at Reason Foundation and a senior economic advisor to Toreador Research & Trading. March 1st 2015. “Why Robots Will Be The Biggest Job Creators In World History,” *Forbes*, <http://www.forbes.com/sites/johntamny/2015/03/01/why-robots-will-be-the-biggest-job-creators-in-history/#6fce3cc51749>. Accessed October 28th 2016) ESG

**Robots will ultimately be the biggest job creators simply because aggressive automation will free us up to do new work by virtue of it erasing toil that was once essential.** Lest we forget, there was a time in American history when just about everyone worked whether they wanted to or not — on farms — just to survive. Thank goodness technology destroyed lots of agricultural work that freed Americans up to pursue a wide range of vocations off the farm. **With their evolution as labor inputs, robots bring the promise of new forms of work that will have us marveling at labor we wasted in the past**, and that will make past job destroyers like wind, water, the cotton gin, the car, the internet and the computer seem small by comparison. All the previously mentioned advances made lots of work redundant, but far from forcing us into breadlines, **the destruction of certain forms of work occurred alongside the creation of totally new ways to earn a living. Robots promise a beautiful multiple of the same.**

#### 4. Even with automation, people are needed for operation

The Economist (The Economist, English-language weekly newspaper owned by the Economist Group and edited in offices based in London. Apr 21st 2012. “Making the future” *The Economist*, <http://www.economist.com/node/21552897>) ESM

Yet manufacturing will still need people, if not so many in the factory itself. All these automated machines require someone to service them and tell them what to do. Some machine operators will become machine minders, which often calls for a broader range of skills. And certain tasks, such as assembling components, remain too fiddly for robots to do well, which is why assembly is often subcontracted to low-wage countries. Industrial robots are getting better at assembly, but they are expensive and need human experts to set them up (who can cost more than the robot). They have a long way to go before they can replace people in many areas of manufacturing.Investing in robots can be worthwhile for mass manufacturers like carmakers, who remain the biggest users of such machines, but even in highly automated car factories people still do most of the final assembly. And for small and medium-sized businesses robots are generally too costly and too inflexible.

#### **5.** Even if they are correct, automation may create universal basic income

**Nickolaus Hines, 2016** (Nicklaus Hines, author for *Inverse.* August 11th 2016. “Robots Could Make Universal Basic Income a Necessity,” *Inverse,* <https://www.inverse.com/article/18443-automation-will-make-universal-basic-income-a-necessity>.Accessed Nov 19 2016) ESG

On July 5, the White House hosted a Facebook Live roundtable with technology entrepreneur Robin Chase and author Martin Ford. Chase and Ford focused on the state of employment in the United States, and the growing effects of automation. They didn’t bother discussing which political party would bring more jobs back, or how other countries are stealing America’s jobs, but they did say universal basic income was America’s best chance to survive an automated future. Chase and Ford aren’t the first to discuss a UBI program in the United States either. President Richard Nixon briefly championed a version of guaranteed income before social and political pressures turned him off of the idea. Yet technological automation is a major force present in modern talks about universal basic income that Nixon didn’t have to contend with. **Technology doesn’t care what race you are, or whether you’re a blue collar or white collar worker. In a way, automation is the great equalizer, and it may be enough to make UBI an inescapable reality.**

### AT: AI Bad

#### 1. AI is advancing, but it does *not* have the capabilities needed to become malevolent

**Rodney Brooks, 2014** (Rodney Brooks, founding director of MIT’s Computer Science and Artificial Intelligence Laboratory. November 10th 2014. “Artificial Intelligence is a Tool, Not a Threat,” *Rethink Robotics*, <http://www.rethinkrobotics.com/blog/artificial-intelligence-tool-threat/>. Accessed 10/28/2016) ESG

I think **it is a mistake to be worrying about us developing malevolent AI anytime in the next few hundred years.** I think the worry stems from a fundamental error in not distinguishing the difference between the very real recent advances in a particular aspect of AI, and the enormity and complexity of building sentient volitional intelligence. **Recent advances in deep machine learning let us teach our machines things like how to distinguish classes of inputs and to fit curves to time data.** This lets our machines “know” whether an image is that of a cat or not, or to “know” what is about to fail as the temperature increases in a particular sensor inside a jet engine. **But this is only part of being intelligent**, and Moore’s Law applied to this very real technical advance will not by itself bring about human level or super human level intelligence. While deep learning may come up with a category of things appearing in videos that correlates with cats, it doesn’t help very much at all in “knowing” what catness is, as distinct from dogness, nor that those concepts are much more similar to each other than to salamanderness. **And deep learning does not help in giving a machine “intent”, or any overarching goals or “wants”.** And it doesn’t help a machine explain how it is that it “knows” something, or what the implications of the knowledge are, or when that knowledge might be applicable, or counterfactually what would be the consequences of that knowledge being false. Malevolent AI would need all these capabilities, and then some. Both an intent to do something **and an understanding of human goals, motivations, and behaviors would be keys to being evil towards humans.**

#### 2. Artificial intelligence may help hone human intelligence and skills

**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.

That concern aside, Kelly believes that **AI will help make humans smarter and more effective.** He notes, **for example, that AI chess programs have helped make human chess players much better**. He adds, **“If AI can help humans become better chess players, it stands to reason that it can help us become better pilots, better doctors, better judges, better teachers.”** In other words, Kelly seesAI as toolthat **can help mankind get better not a threat that is going to destroy mankind.** He continues: “Most of the commercial work completed by AI will be done by special-purpose, narrowly focused software brains that can, for example, translate any language into any other language, but do little else. Drive a car, but not converse. Or recall every pixel of every video on YouTube but not anticipate your work routines. In the next 10 years, 99 percent of the artificial intelligence that you will interact with, directly or indirectly, will be nerdily autistic, supersmart specialists. In fact, this won’t really be intelligence, at least not as we’ve come to think of it. Indeed, intelligence may be a liability — especially if by ‘intelligence’ we mean our peculiar self-awareness, all our frantic loops of introspection and messy currents of self-consciousness.”

#### In fact, intentionally evil AI is likely *centuries* away

**Rodney Brooks, 2014** (Rodney Brooks, founding director of MIT’s Computer Science and Artificial Intelligence Laboratory. November 10th 2014. “Artificial Intelligence is a Tool, Not a Threat,” *Rethink Robotics*, <http://www.rethinkrobotics.com/blog/artificial-intelligence-tool-threat/>. Accessed 10/28/2016) ESG

Expecting more computation to just magically get to intentional intelligences, who understand the world is similarly unlikely. And, there is a further category error that we may be making here. That is the intellectual shortcut that says computation and brains are the same thing. Maybe, but perhaps not. In the 1930’s Turing was inspired by how “human computers”, the people who did computations for physicists and ballistics experts alike, followed simple sets of rules while calculating to produce the first models of abstract computation. In the 1940’s McCullough and Pitts at MIT used what was known about neurons and their axons and dendrites to come up with models of how computation could be implemented in hardware, with very, very abstract models of those neurons. Brains were the metaphors used to figure out how to do computation. Over the last 65 years those models have now gotten flipped around and people use computers as the metaphor for brains. So much so that enormous resources are being devoted to “whole brain simulations”. I say show me a simulation of the brain of a simple worm that produces all its behaviors, and then I might start to believe that jumping to the big kahuna of simulating the cerebral cortex of a human has any chance at all of being successful in the next 50 years. And then only if we are extremely lucky. **In order for there to be a successful volitional AI, especially one that could be successfully malevolent, it would need a direct understanding of the world, it would need to have the dexterous hands and/or other tools that could out manipulate people, and to have a deep understanding of humans in order to outwit them. Each of these requires much harder innovations than a winged vehicle landing on a tree branch. It is going to take a lot of deep thought and hard work from thousands of scientists and engineers. And, most likely, centuries.**

#### 3. Turn: AI has a variety of benefits:

#### AI could help predict earthquakes faster

Elgan 16(Mike Elgan, columnist at Computerworld.com and former chief editor for multiple big tech magazines, February 22nd 2016, Computerworld.com, “Artificial intelligence needs your data, all of it,” <http://www.computerworld.com/article/3035595/emerging-technology/artificial-intelligence-needs-your-data-all-of-it.html> DoA: 10/26/16) CJV

Another research project out of the University of California at Berkeley last week published a free app called [MyShake](http://www.dailycal.org/2016/02/17/uc-berkeley-researchers-create-smartphone-app-detect-earthquakes/%22%20%5Ct%20%22new) that can detect earthquakes. It uses the motion sensors in smartphones to constantly monitor the phones' every movements. The app can tell when motion is caused by an earthquake or from non-earthquake motion. It's like having millions of seismographs all over the place, rather than dozens or hundreds. Eventually, the system should be able to predict earthquakes faster than current systems.

#### AI could help the visually impaired

Elgan 16(Mike Elgan, columnist at Computerworld.com and former chief editor for multiple big tech magazines, February 22nd 2016, Computerworld.com, “Artificial intelligence needs your data, all of it,” <http://www.computerworld.com/article/3035595/emerging-technology/artificial-intelligence-needs-your-data-all-of-it.html> DoA: 10/26/16) CJV

And yet another new app came out recently for iOS that helps visually impaired people to identify everyday objects. To use it, you simply snap a picture. Artificial intelligence in the cloud analyzes the smartphone photo, figures out what it is, then sends the answer back. For example, let's say a blind user is shopping for a birthday present at Toys 'R' Us. The user points the camera at a box, and has [Aipoly](http://aipoly.com/%22%20%5Ct%20%22new) tell the user that it's a Star Wars Lego set. Or while shopping for fruit, the app could tell the difference between a lemon and a lime. The app works because volunteer users who are not visually impaired snap pictures of random objects and identify them for the system. Aipoly doesn't work perfectly. But it could if it had enough data.

### AT: Smart Cities Bad

#### 1. Smart Cities can spur innovation

Christos Cassandras 2016 (Christos G. Cassandras, Division of Systems Engineering & Center for Information and Systems Engineering, Boston University. 30 June 2016 “Smart Cities as Cyber-Physical Social Systems” from Elsevier Journal. PDF. DOA: 10/20/16. P.158) ESM

(2) The “law of unintended consequences” finds fertile ground in smart cities. When people are provided with an abundance of new data and services, they exhibit an amazing capacity to use services developed for specific purposes in innovative ways that were never envisioned in the first place. This principle of beneficial “unintended consequences” appears to be at work when one continuously develops new capabilities and makes them widely available in simple, intuitive, easy-to-use ways. Thus, creating a few apps and establishing a user-friendly platform for accumulating and disseminating data has a remarkable amplification capability in promoting innovation.

#### **2.** IoT systems saved 58 million on water, 50 million on parking, and 37 million on smart lighting

**Laura Adler 2016** (Laura Adler is a PhD student in Sociology at Harvard. She received a Bachelors from Yale University and a Masters in City Planning from the University of California, Berkeley. February 18, 2016. “How Smart City Barcelona Brought the Internet of Things to Life,” Data-Smart City Solutions. <http://datasmart.ash.harvard.edu/news/article/how-smart-city-barcelona-brought-the-internet-of-things-to-life-789> DOA: 10/31/16) CDY

**Already, these improvements have saved the city money and reduced the consumption of valuable energy and water. [Barcelona estimates](http://www.forbes.com/sites/connieguglielmo/2014/01/07/ces-live-cisco-ceo-chambers-to-deliver-keynote/%22%20%5Ct%20%22_blank) that IoT systems have helped save $58 million on water, increased parking revenues by $50 million per year, and generated 47,000 new jobs. Through smart lighting, the city reports saving an addition $37 million annually**. To capitalize on the energy around the city’s IoT projects, Barcelona has actively fostered its local technology industry. With $230 million in public funds, the [city redeveloped an industrial area](http://www.technologyreview.com/news/532511/barcelonas-smart-city-ecosystem/%22%20%5Ct%20%22_blank) to create [22@Barcelona](http://www.22barcelona.com/%22%20%5Ct%20%22_blank), where startups are putting public data to use in new applications and developing IoT technologies. Among these startups is [thethings.io](http://thethings.io/%22%20%5Ct%20%22_blank), which aims to become the primary service provider for the IoT world. Some of these homegrown companies are already starting to find market success. One 22@Barcelona resident, [Worldsensing](http://www.worldsensing.com/%22%20%5Ct%20%22_blank), developed an in-ground parking sensor that cities can use to manage citizen parking. Barcelona piloted the tool, [Fastprk](http://www.fastprk.com/%22%20%5Ct%20%22_blank), in the 22@Barcelona district, helping the product evolve through a real-world implementation. While Barcelona ultimately purchased a different tool for broader implementation, Fastprk is finding a market, with 10,000 units installed in Moscow. In addition to fostering local companies, 22@Barcelona is attracting private investment. Cisco announced plans to invest $30 million in a new center focused on the Internet of Everything (IoE). For Cisco, this will be the third IoE innovation center, following developments in Brazil and South Korea, thus establishing Barcelona as a leader on the European continent.

#### **3.**

### AT: Hurts Small Business

#### 1. **IoT is well within reach for small businesses**

Xander Schofield 2016 ([Xander Schofield](https://datafloq.com/read/author/xander-schofield/688), IT Consultant 2016 “How IoT Devices Will Help Small Businesses Work Smarter” from Datafloq. <https://datafloq.com/read/IoT-devices-help-small-businesses-work-smarter/2207> DOA: 11/4/16) ESM

The Internet of Things, commonly abbreviated as IoT, is a term used to describe the vast network of internet-enabled devices and sensors that are revolutionizing the way we do business in the 21st century. The term was coined in 1999 in reference to RFID chips, but in recent years the state of IoT has advanced exponentially beyond to achieve greater and greater possibilities. The smartphone is one early example of an IoT device, especially as it becomes more and more ubiquitous in society. There are also a whole host of new technologies in development that allow small, low cost devices to perform a range of automated, context sensitive tasks over WiFi Internet. IoT is being quickly being capitalized on by large businesses, but it is certainly not out of reach of the average small business. In fact, small businesses can increase their chance of success by a large margin when they delve into the world of IoT. Discover the many ways that this new paradigm can improve daily operations with the following relevant applications.

#### 2. **IoT allows small businesses to become more effective with smart tech**

Esther Shein 2015 (Esther Shein, freelance writer and editor for Forbes. DEC 14, 2015 “How The Internet Of Things Is Helping Small Businesses” from Forbes. <http://www.forbes.com/sites/centurylink/2015/12/14/how-the-internet-of-things-is-helping-small-businesses/#3768a78859fe> DOA: 11/3/16) ESM

IoT can also help small businesses become more efficient and effective in their day-to-day operations. “As IoT systems’ costs come down, displacement of traditional systems could reduce operating expenses,” said [Michael Feldman](https://protect-us.mimecast.com/s/MdRlBYs0qZWUw%22%20%5Ct%20%22_blank), an IoT product engineering consultant and former vice president of engineering at Bigbelly Solar. Small businesses can use IoT-based security alarm systems and other sensor-based systems such as IoT thermostats and air-conditioning systems to help control heat and electricity costs, he said. Some 57 percent of small businesses expect IoT to have a significant impact on their bottom line, according to a 2014 study by the security software company [AVG](http://now.avg.com/businesses-expect-iot-profits/%22%20%5Ct%20%22_blank). “By remotely monitoring the data on these devices, a business can achieve much greater all-around efficiency through raised productivity, lower costs and reduced wastage,’’ the authors of AVG’s study noted. “And as cloud services become the default way to make sense of this data, you no longer need heavy up-front investment, so IoT starts to become affordable for small businesses.”

#### 3. **IoT will reduce operating costs, increase productivity and expand markets, helping small businesses**

Andrew Meola 2016 ([Andrew Meola](http://www.businessinsider.com/author/andrew-meola), writer for [BI Intelligence](https://intelligence.businessinsider.com/?IR=T&utm_source=businessinsider&utm_medium=content_marketing&utm_term=content_marketing_bio_page&utm_content=content_marketing_bio_page&utm_campaign=content_marketing_bio_page" \t "_blank), Business Insider's premium research service. Sep. 2, 2016 “IoT for Small Business: Effects, Opportunities & Platforms” from Business Insider <http://www.businessinsider.com/internet-of-things-small-business-opportunities-platforms-2016-8> DOA:10/24/16)ESM

And as the IoT expands, it will have a particularly profound effect on businesses, especially small businesses. Several IoT business opportunities will be created in the coming years as we head into an increasingly connected world.Below, we've compiled a detailed rundown of new IoT business platforms and the potential those platforms will create in the near future. Effects of IoT on Small Businesses Businesses will be the top adopter of IoT solutions in the next few years. And this will create tremendous benefits for the businesses that choose to wholeheartedly embrace this growing trend, as there are three ways the IoT can improve their bottom line: 1) reduce operating costs; 2) increasing productivity; and 3) expanding to new markets or developing of new product offerings. BI Intelligence expects that from 2015 to 2020, business investments in the IoT will grow from $215 billion to $832 billion. This is just one slice of the overall pie, as compounded, we project more than $6 trillion will be spent on IoT solutions between 2015 and 2020 among businesses, consumers, and governments.

#### **He continues,**

Andrew Meola 2016 ([Andrew Meola](http://www.businessinsider.com/author/andrew-meola), writer for [BI Intelligence](https://intelligence.businessinsider.com/?IR=T&utm_source=businessinsider&utm_medium=content_marketing&utm_term=content_marketing_bio_page&utm_content=content_marketing_bio_page&utm_campaign=content_marketing_bio_page" \t "_blank), Business Insider's premium research service. Sep. 2, 2016 “IoT for Small Business: Effects, Opportunities & Platforms” from Business Insider <http://www.businessinsider.com/internet-of-things-small-business-opportunities-platforms-2016-8> DOA:10/24/16)ESM

It's clear that the IoT will affect small businesses, but how will those changes manifest? There is no shortage of devices that small businesses can leverage in order to take advantage of the IoT. Smart locks from companies such as August, for example, can give small businesses peace of mind and help their wallets by circumventing the need to hire security guards. To take this a step further, companies can purchase connected cameras to monitor their offices in real time. Another popular device is the mobile credit card reader that connects to smartphones and tablets. Square is the household name in this regard, as businesses from food trucks to flea markets use the card reader to process transactions easily. And if you need to keep track of shipped products, smart fleet trackers can save time and money and reduce customer frustration.

#### 4. IOT can reduce fraud and promote quality products for businesses

**Daniele Miorandi et al, 2012,** [Daniele Miorandi et. Al, April 2012, The head of the iNSPIRE Area at CREATE-NET, Italy. He received a PhD in Communications Engineering from Univ. of Padova, Italy, “Internet of things: Vision, applications and research challenges,” pg, 1511, <https://irinsubria.uninsubria.it/retrieve/handle/11383/1762288/2389/IOT.pdf>, DOA: 10/15/16, AA]

Smart business/Inventory and product management. RFID technologies are already used in many sectors for inventory management, throughout the supply and delivery chain. This relies on the ability of RFID technologies to identify and provide support for tracking goods. At the moment, however, RFID applications are built in a rather ad hoc fashion, and are only partially integrated into supply management systems. RFID are customarily used to monitor and manage the movement of products through a supply chain; typically, RFID tags are directly attached to the items (or to the containers that carry them), while readers are placed throughout the facility to be monitored. IoT technologies can provide enhanced flexibility in terms of readers positions, while at the same time enabling seamless interoperability between RFID-based applications used by different actors dealing with the product throughout the various phases of its life-cycle. In retail applications, **IoT technologies can be used to monitor in real-time product availability and maintain accurate stock inventory.** They can also play a role in after-market support, whereby users can automatically retrieve all data about the products they bought. Also, **identification technologies can help in limiting thefts and in fighting counterfeiting by providing products with a unique identifier including a complete and trustworthy description of the good itself.** Furthermore, sensors and specifically bio-sensor technologies in combination with RFID technology may allow control production processes, final product quality and possible shelf life deterioration of the product, e.g., in the food industry. For example, RFID devices can be used to identify and track the product, while the bio-sensors can monitor parameters such as temperature and bacterial composition in order to guarantee required quality of the final product.

### AT: Autocratic Regimes

#### 1. **Iot has the potential to increase democratic engagement**

Phillip Howard, 2016 (Phillip Howard, writer for the Brookings Institute, March 4, 2016 “Idea to retire: A closed-platform Internet of Things” <https://www.brookings.edu/blog/techtank/2016/03/04/idea-to-retire-a-closed-platform-internet-of-things/> DOA: 10/19/16) F.K

After that, we need to make sure the IoT is built for civic engagement, not simply government policymaking and industry marketing. These days, it’s normal for civil-society groups to have an Internet strategy or a social media strategy. It’s not too soon for them to consider their IoT strategy. The next Internet is still far enough away that citizens can have a voice in how it is constructed and operated. To shape the next Internet responsibly and wisely, citizens will have to understand what the IoT truly will be—an information infrastructure for public life and civic virtue. And there are several things we can do now to build political participation into IoT. With billions of sensors to learn from, there’s no reason governments shouldn’t use them to make better public policy. And firms should be allowed to do in-depth market research on the behavior of their customers and use smart devices to run their business efficiently. It’s very likely that citizens and consumers will benefit from IoT innovations, but policymakers have to let go of the idea that the Internet is made up of cellphones and laptops.  First and foremost, they must provide ways to ensure that people are presented with choices about who gets to use their individual data for politics.  And they have to treat device networks as common carriers for the public good.

#### 2. The IoT can create democracy and openness

**Phil Howard et al, 2016** (Phil Howard, professor of technology and international affairs at Oxford University, Christopher Walker, VP of Research and Studies at the National Endowment for Democracy, and Mark Nelson, senior director at the Center for International Media Assistance. January 8th 2016. “Will the internet of things enhance democracy or empower autocrats?” *Democracy Digest*, <http://www.demdigest.org/will-the-internet-of-things-enhance-democracy-or-empower-autocrats>. Accessed Nov 10 2016) ESG

What will this omnipresent connectivity mean for the future of democracy? Soon, we will be fully immersed in a pervasive yet invisible network of everyday objects that communicate with one another. There is evidence that in authoritarian countries, the internet of things will be another tool for social control. Even in democracies, the privacy threats are enormous, as is the potential for political manipulation. **Yet we should also imagine a future of global stability built upon device networks with immense potential for empowering citizens, making government transparent, and broadening information access. If we can actively engage with the governments and businesses building the internet of things, we have a chance to build a new kind of internet—and a more open society.**

#### 3. Technology has empowered citizen to amplify their voices and hold governments accountable

**National Democratic Institute** (National Democratic Institute, nonprofit and nonpartisan organization with a focus on democracy. N/D. DOA: November 11, 2016. “Technology Is Transforming Democracy,” National Democratic Institute. <https://www.ndi.org/technology-transforming-democracy>) EL

**Innovations in technology and social media have had a significant impact on democracy globally. Technology has empowered citizens to amplify their voices and hold governments accountable.** But while citizens have begun to harness tech innovation, many democratic institutions — governments, parliaments and political parties — have been slower to react, often using outmoded processes to respond to increased citizen demands. [Read more about NDI's approach to technology and democracy»](https://www.ndi.org/democracy-and-technology)

#### 4. The Internet of Things decentralizes power

**Lawrence Ampofo 2016** (Lawrence Ampofo, political scientist and strategic communications consultant for Semantica Research. February 2nd 2016. “How the Internet of Things Influences Democracy,” *Semantica Research*, <http://www.semanticaresearch.com/how-the-internet-of-things-influences-democracy/>. Accessed Nov 12th 2016) ESG

**The Internet of Things has the potential to vastly strengthen the democratic values and institutions that together form the bedrock of Western civilisation. Collectively, these technologies facilitate the movement of social and political power from the ‘centre to the edges’.** However, in order for this vision of our connected future to come to pass, people have to demand the same level of disclosure and transparency of data from hitherto powerful institutions as they currently do from us. **The most successful companies in the age of the Internet of Things (IoT) will created products and services that are at once hyperpersonal, transparent and take to heart the protection of individual privacy and security.** The Internet and the World Wide Web have strengthened democratic values, so it has been claimed. By providing everyone connected to the network the opportunity to share their voice, the Internet and the Web become the digital embodiment of one of the great achievements of democracy; the ability for people to contribute their voice to global society. People now, to a greater or lesser extent, can share anything, anywhere at any time.

#### 5. Surveillance fails—the data just isn’t useful to law enforcement

**Marshall Erwin 2016** (Marshall Erwin, senior staff analyst; 4/17/16; "The Internet-of-Things-That-Are-Marginally-Useful-for-Surveillance" The Cipher Brief; DOA: 11/12/16; <https://www.thecipherbrief.com/article/techcyber/internet-things-are-marginally-useful-surveillance-1092>) AM

**The Internet-of-Things** has for years promised to usher in a new wave of innovation. It has sometimes been called the Internet-of-Everything or Internet 3.0—grand language illustrating its potential. That potential would also seem to offer new opportunities for law enforcement and intelligence services. But the promise has thus far not materialized. I prefer, somewhat glibly, to use my own term for this wave of technological change: the Internet-of-Things-That-Are-Marginally-Useful-for-Surveillance (IOTTAMUFS). I use this term because the IOTTAMUFS **is not going to be the boon to law enforcement and intelligence services that [some suggest](https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf%22%20%5Ct%20%22_blank).** Here is why. The IOTTAMUFS presents two fundamental privacy and security challenges. First the privacy problem: consumers have no ability to understand the way in which IOTTAMUFS devices will collect and use data about them. As a result, they can’t provide meaningful consent to the collection. This problem already exists across the Internet today, but when consumers visit a website or use their iPhone, many at least have some idea that data collection is occurring in the background. That isn’t the case when everyday devices, like refrigerators or thermostats, collect data. Second, the security problem: for these everyday devices, it is going to be difficult to update or patch software or even to build strong security in the first place. As a result, many are going to be extremely vulnerable to compromise. A consumer privacy problem coupled with a product security problem are the two most fundamental ingredients for a surveillance opportunity, whether that surveillance is carried out by an intelligence agency, law enforcement, or a malicious hacker. And as privacy and security issues go, these two problems are massive. Industry isn’t anywhere close to figuring out how to solve them. But **much of the data that is going to be collected by these everyday devices—and potentially going to be available for surveillance purposes—just isn’t going to be that useful. It is low value data. The data likely to be exposed isn’t often going to be data that intelligence and law enforcement agencies actually want.** I agree with the general argument made in the recent encryption debate that law enforcement has access to huge amounts of data today that can allow it to compensate for a lose of access due to encryption. But this argument rests on an assumption that isn’t always true – that the data law enforcement is gaining access to is as valuable for investigative purposes as the access it is losing. In some cases, such as the growing volume of geolocation data available, the argument holds up. In other cases, such as the IOTTAMUFS, it might not. For example, consider data collected and used by the adtech industry. The Internet has brought a revolution to the advertising industry that is as consequential as the rise of the iPhone. Ad tech companies now collect vast amounts of data about Internet users that can be used to build consumer profiles and target advertising. The scope of this collection is staggering. However, **despite the quantities of that data collected, this revolution in technology has not been nearly as consequential to law enforcement.** The data in question simply isn’t that valuable outside of the context in which it is collected and used. The same is going to be true for much of the data collected by IOTTAMUFS devices. **The data from your thermostat or refrigerator just isn’t going to be as valuable as the data on your phone**. What does this mean for the privacy and security challenges mentioned earlier? It means that the **surveillance opportunities** created by these two fundamental problems **are only going to be useful in a small number of cases, involving extremely motivated attackers targeting key individuals.** It is only in those cases where someone will invest the time and effort to exploit vulnerabilities in IOTTAMUFS devices and figure out how to derive some value out of large quantities of mostly useless data. **These new devices will create opportunities to collect information about heads of state but won’t be as helpful when it comes to standard criminals or lower level intelligence targets.** This is consistent with the general tend that we’ve seen in recent years and that is likely to continue: highly targeted surveillance that takes longer to execute will become easier even while quick, more broadly applicable surveillance becomes harder. Simply put, the attack surface for the products and systems we use has broadened and diversified. And while this provides an abundance of niche opportunities, it also means that there will be fewer simple surveillance solutions in the future.

#### 6. Democracy has only grown in spite of surveillance tech

**Max Roser 2016**(Max Roser, an economist at Oxford University; 2016; "Democracy"; Our World In Data; doa: 11/18/16;[https://ourworldindata.org/democracy/](https://ourworldindata.org/democracy/%22%20%5Ct%20%22_blank)) AM

**A democracy is a political system with institutions that allows citizens to express their political preferences, has constraints on the power of the executive, and a guarantee of civil liberties.** This entry presents the empirical research on the slow rise of democratic regimes over the last two centuries. Democracies are distinct from autocratic countries in which political preferences cannot be expressed and citizens are not guaranteed civil liberties. Anocracies – a term used often in this entry – are regimes that fall in the middle of the spectrum of autocracies and democracies. Anocracies are countries which are not fully autocratic, but which can also not be called democratic. **The majority of the world’s countries are now governed by democratic regimes**, defined as systems with citizen political participation, constraints on the power of the executive, and a guarantee of civil liberties. The visualization below shows the slow **increase of democratic countries** over the last 200 years. The rise of democracies has been interrupted by the atrocities during the two World Wars – many young democracies fell back to become autocratic ahead of the Second World War.After 1945 the number of democracies has started to grow again, but**the very dramatic shift towards a democratic world has been** the breakdown of the Soviet Union **in 1989**. By clicking on ‘Autocracies’ and ‘Anocracies’, you can also see that after 1989 the number of autocracies has decreased dramatically while the number of anocracies initially increased then has stayed fairly stable.

### AT: Hacking

#### 1. We’re already solving for cybersecurity in the real world.

Jason Lange 2016 (Jason Lange, columnist covering economics and the Federal Reserve for Reuters, October 11th 2016, *Reuters*, “G7 sets common cyber-security guidelines for financial sector,” <http://www.reuters.com/article/us-cyber-g-idUSKCN12B1UB> DoA: 11/3/16) CJV

The Group of Seven industrial powers on Tuesday said they had agreed on guidelines for protecting the global financial sector from cyber attacks following a series of cross-border bank thefts by hackers. Policymakers have grown more worried about financial cyber security in the wake of numerous hacks of SWIFT, the global financial messaging system, including an $81 million theft in February from the Bangladeshi central bank’s account at the New York Federal Reserve. “Cyber risks are growing more dangerous and diverse, threatening to disrupt our interconnected global financial systems,” according to the guidelines agreed by G7 finance ministers and central bankers. The guidelines, which officials described as non-binding principles, were in a three-page document posted on the Web pages of G7 government agencies. The G7 comprises Britain, Canada, France, Germany, Italy, Japan and the United States. U.S. Deputy Treasury Secretary Sarah Bloom Raskin told reporters in a telephone briefing that G7 officials had surveyed their existing cyber security practices and identified potential shortfalls. A Treasury official later said the guidance was an effort to encourage regulators and firms to approach cyber security from a risk-management perspective. Fed Vice Chairman Stanley Fischer said in a statement the guidelines would address the weakest links in global cyber security.

#### 2. Not unique to IoT - Most cyberattacks are due to mistakes by idiots, not hackers

Joseph Menn 2015 (Joseph Menn, writer for Reuters, April 14th 2015, *Insurance Journal*, “Most Cyber Attacks Due to Trick Emails, Errors, Not Sophisticated Hacking,” <http://www.insurancejournal.com/news/national/2015/04/14/364191.htm>, DoA: 11/3/16) CJV

When a cyber security breach hits the news, those most closely involved often have incentive to play up the sophistication of the attack. If hackers are portrayed as well-funded geniuses, victims look less vulnerable, security firms can flog their products and services, and government officials can push for tougher regulation or seek more money for cyber defenses. But two deeply researched reports being released this week underscore the less-heralded truth: the vast majority of hacking attacks are successful because [employees click on links in tainted emails](http://www.insurancejournal.com/news/national/2015/02/10/357051.htm%22%20%5Ct%20%22_blank%22%20%5Co%20%22Investigators%20Suspect%20Anthem%20Breach%20Began%20with%20%27Phishing%27%20of%20Employees), companies fail to apply available patches to known software flaws, or technicians do not configure systems properly. These conclusions will be in the minds of executives attending the world’s largest technology security conference next week in San Francisco, a conference named after lead sponsor RSA, the security division of EMC Corp. In the best-known annual study of data breaches, a report from Verizon Communications Inc. to be released on Wednesday found that more than two-thirds of the 290 electronic espionage cases it learned about in 2014 involved phishing, the security industry’s term for trick emails. Because so many people click on tainted links or attachments, sending phishing emails to just 10 employees will get hackers inside corporate gates 90 percent of the time, Verizon found. “There’s an overarching pattern,” said Verizon scientist Bob Rudis. Attackers use phishing to install malware and steal credentials from employees, then they use those credentials to roam through networks and access programs and files, he said.

#### 3. Privacy enhancing technology can help solve

Alex Bassi 2012 (Alex Bassi, the chair from 2007 until 2013 of the European Technology Platform on Smart Systems Integration "EPoSS" RFID / Internet of Things Working Group; currently, he is the co-chair of the Manufacturing WG. Rob van Kranenburg, He is co-founder of [bricolabs](http://bricolabs.net/%22%20%5Ct%20%22_blank) and the founder of [Council](http://blog.theitjobboard.co.uk/6-communities-internet-things-professionals/%22%20%5Ct%20%22_blank), author of several books on IoT. 2012. “IoT Challenges” from Communications in Global Commuting, Springer Open Journal. <http://muxjournal.springeropen.com/articles/10.1186/2192-1121-1-9> DOA: 10/17/16. P.3) ESM

Privacy was named by the originator of ubicomp, Mark Weiser, the late chief scientist at Xerox Parc as a key issue (Weiser, 1991) [3]. Machina Research, in association with Latitude, Council and Info.nl – a trio of web 2.0 consultancy companies – recently ran an web survey, polling views on the future internet of things. One of the questions was related to concerns that people may have about living in a future connected environment. Privacy was mentioned by a clear majority as a key challenge. Privacy Enhancing Technologies (PET) is a partial solution. The Privacy Coach, [4] produced by a small Dutch consortium of RFID experts, is an application running on a mobile phone that supports customers in making privacy decisions when confronted with RFID tags (Broeninjk and others, 2011). It functions as a mediator between customer privacy preferences (Fischer-Hübner, 2011) and corporate privacy policies, trying to find a match between the two, and informing the user of the outcome. Gérald Santucci (head of unit Knowledge Sharing), key IOT architect at the European Commission explains: "in the future, the right to privacy, whatever we do to implement it with technology and/or regulations ("right to be forgotten", "right to oblivion", "right to silent chips", etc.), will become a subset of ethics. The future is (largely) about ethics-by-design” [5].

#### 4. **AES will be used to protect information**

Naofumi Homma 2016 (Naofumi Homma, Lightweight Cryptography WG Member, American Association for the Advancement of Science  22-AUG-2016 “World's most efficient AES crypto processing technology for IoT devices developed” from EurekAlert!, a part of the American Association for the Advancement of Science. <https://www.eurekalert.org/pub_releases/2016-08/tu-wme082216.php> DOA: 10/28/16) ESM

Our research group has discovered a new technique for compressing the computations of encryption and decryption operations known as Galois field arithmetic operations, and has succeeded in developing the world's most efficient Advanced Encryption Standard (AES) cryptographic processing circuit, whose energy consumption is reduced by more than 50% of the current level. With this achievement, it has become possible to include encryption technology in information and communication technology (ICT) devices that have tight energy constraints, greatly enhancing the safety of the next-generation Internet of Things (IoT). This result was announced on August 19, 2016 during the Conference on Cryptographic Hardware and Embedded Systems 2016 (CHES 2016) hosted by the International Association for Cryptologic Research (IACR) in Santa Barbara, USA. Social background of this development: It is currently very common to exchange important personal or financial information over the Internet through ICT devices. Cryptographic techniques are used inside these devices to protect important information. In next-generation networks such as the IoT, which has attracted attention in recent years, it is expected that myriad devices will be connected to the network. Hence, it will be necessary to have built-in encryption technology in these connected devices to prevent malicious attacks. However, many battery or cell-driven devices with tight energy constraints are also included in the IoT and running energy-consuming encryption processes on these is a big challenge. One of the most widely used international standard encryption methods is AES. Since this is used in areas such as wireless LANs, it is very important for practical reasons to design energy-saving AES cryptographic processing.

#### 5. Artificial intelligence can help mitigate cybercrime

Tarun 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

As threats grew even more complicated and targeted, businesses and governments should take every available opportunity to learn more about the most advanced and cost effective bespoke security solutions. **Artificial intelligence hasn't just strengthened the IoT, it's also very effective while detecting and combating the security threats because identifying online minuscule shifts is easier for AI-based technologies than the conservative approaches. Researchers at MIT's Computer Science and CSAIL achieved a big breakthrough when they developed an AI-based system which is capable of detecting 85 percent of threats from more than 3.6 billion log files each day.** With the help of Big Data Analytical tools, AI helps to read and study the changing behaviour of the internet users and whenever a noticeable deviation occurs, it either blocks the threat or issues warning to the main server where the security team takes appropriate actions very promptly. Now, security analysts don't just address the specific problem/threat, but they also take actions to discover other potential threats of shared characteristics. Simultaneously, they anticipate a problem and resolve it with customised security solutions. And, recent developments in the robotic engineering have supported well in strengthening the AI against IoT threats.

### AT: Security Harms General

#### 1. Privacy enhancing technology can help solve

Alex Bassi 2012 (Alex Bassi, He was the chair from 2007 until 2013 of the European Technology Platform on Smart Systems Integration "EPoSS" RFID / Internet of Things Working Group; currently, he is the co-chair of the Manufacturing WG. Rob van Kranenburg, He is co-founder of [bricolabs](http://bricolabs.net/%22%20%5Ct%20%22_blank) and the founder of [Council](http://blog.theitjobboard.co.uk/6-communities-internet-things-professionals/%22%20%5Ct%20%22_blank), author of several books on IoT. 2012. “IoT Challenges” from Communications in Global Commuting, Springer Open Journal. <http://muxjournal.springeropen.com/articles/10.1186/2192-1121-1-9> DOA: 10/17/16. P.3) ESM

Privacy was named by the originator of ubicomp, Mark Weiser, the late chief scientist at Xerox Parc as a key issue (Weiser, 1991) [3]. Machina Research, in association with Latitude, Council and Info.nl – a trio of web 2.0 consultancy companies – recently ran an web survey, polling views on the future internet of things. One of the questions was related to concerns that people may have about living in a future connected environment. Privacy was mentioned by a clear majority as a key challenge. Privacy Enhancing Technologies (PET) is a partial solution. The Privacy Coach, [4] produced by a small Dutch consortium of RFID experts, is an application running on a mobile phone that supports customers in making privacy decisions when confronted with RFID tags (Broeninjk and others, 2011). It functions as a mediator between customer privacy preferences (Fischer-Hübner, 2011) and corporate privacy policies, trying to find a match between the two, and informing the user of the outcome. Gérald Santucci (head of unit Knowledge Sharing), key IOT architect at the European Commission explains: "in the future, the right to privacy, whatever we do to implement it with technology and/or regulations ("right to be forgotten", "right to oblivion", "right to silent chips", etc.), will become a subset of ethics. The future is (largely) about ethics-by-design” [5].

#### 2. **AES will be used to protect information**

Naofumi Homma 2016 (Naofumi Homma, Lightweight Cryptography WG Member, American Association for the Advancement of Science  22-AUG-2016 “World's most efficient AES crypto processing technology for IoT devices developed” from EurekAlert!, a part of the American Association for the Advancement of Science. <https://www.eurekalert.org/pub_releases/2016-08/tu-wme082216.php> DOA: 10/28/16) ESM

Our research group has discovered a new technique for compressing the computations of encryption and decryption operations known as Galois field arithmetic operations, and has succeeded in developing the world's most efficient Advanced Encryption Standard (AES) cryptographic processing circuit, whose energy consumption is reduced by more than 50% of the current level. With this achievement, it has become possible to include encryption technology in information and communication technology (ICT) devices that have tight energy constraints, greatly enhancing the safety of the next-generation Internet of Things (IoT). This result was announced on August 19, 2016 during the Conference on Cryptographic Hardware and Embedded Systems 2016 (CHES 2016) hosted by the International Association for Cryptologic Research (IACR) in Santa Barbara, USA. Social background of this development: It is currently very common to exchange important personal or financial information over the Internet through ICT devices. Cryptographic techniques are used inside these devices to protect important information. In next-generation networks such as the IoT, which has attracted attention in recent years, it is expected that myriad devices will be connected to the network. Hence, it will be necessary to have built-in encryption technology in these connected devices to prevent malicious attacks. However, many battery or cell-driven devices with tight energy constraints are also included in the IoT and running energy-consuming encryption processes on these is a big challenge. One of the most widely used international standard encryption methods is AES. Since this is used in areas such as wireless LANs, it is very important for practical reasons to design energy-saving AES cryptographic processing.

### AT: Car Hacking

#### 1. Cars are not going to be hacked—it’s near impossible

David Pogue 2016 (David Pogue, tech author and tech journalist for the Scientific American; 10/28/16; “Why Car Hacking Is Nearly Impossible”; The Scientific American; DOA: 11/4/16; <https://www.scientificamerican.com/article/why-car-hacking-is-nearly-impossible/> )AM

But would it have been as frightening if she had mentioned that this kind of hack requires a car with cellular Internet service, that **it had taken a team of researchers years to make it work—and that by then the automaker had fixed the software to make such a hack impossible** for vehicles on the road? Then this, in August: “Two researchers have found that they could plug their laptop into a network cable behind a Tesla Model S's driver's-side dashboard, start the car with a software command, and drive it,” Wired reported. But wouldn't you see that if you were in the driver's seat? **Here's the simple truth. No hacker has ever taken remote control of a stranger's car. Not once.** It's extraordinarily difficult to do. It takes teams working full-time to find a way to do it.\* The journalists should also stop calling the perpetrators “hackers.” These are researchers—the good guys—not evildoers hiding in bunkers somewhere. Every time one of those stories pops up, I feel like pulling up alongside the reporters in my own noncellular 2009 Honda Fit and yelling, “Hack this!” Now let me hasten to say this: car security is serious. Not very many cars have built-in Internet connections today—designed for emergency communication, to bring Internet information to the dashboard or to supply a Wi-Fi signal to passengers in the car—but their number is growing. Researchers' demonstrations have underscored the importance of designing these systems securely—for example, of keeping cars' control circuits separate from the Internet ones. In other words, the industry's concern over hackable cars isn't misplaced. Researchers who try to break in are performing a valuable service in drawing attention to a potential danger. **All three cases** described here **led to prompt software fixes by the carmakers**, **who are keen to avoid their products seeming vulnerable. None of those researchers would be able to repeat their demonstrations today**. Unfortunately, you haven't read the last “you're a sitting duck” hacker story. Connected cars are only part of the larger “Internet of things” movement, in which more everyday objects are being made capable of getting online. Home door locks, lighting systems, coffee makers—designing all of it with excellent security is extremely important, and there will be occasional failures. **Yes, new technology is always a little scary. But let's not exploit that fear. Let's assess the hackable-car threat with clarity, with nuance—and with all the facts.** Today remotely hackable cars are still only a hypothetical threat. It's not one that should keep everyday drivers up at night.

### AT: Grid Collapse

#### 1. Even though attacks on the grid are incredibly common, they have done NO damage

**Tim Sampson, 2013** (Tim Sampson, reporter contributing to *The Daily Dot*. May 23rd 2013. “How serious is the hacking threat to the U.S. power grid?” *The Daily Dot*, <http://www.dailydot.com/layer8/cyberattacks-hacking-us-energy-power-grid/>. Accessed Nov 11 2016) ESG

**The electric grid is the target of numerous and daily cyber attacks**, according to the report. More than a dozen utilities reported 'daily,' 'constant,' or 'frequent' attempted cyber attacks ranging from phishing to malware infection to unfriendly probes. **One utility reported that it was the target of approximately 10,000 attempted cyber attacks each month.** More than one public power provider reported being under a 'constant state of attack from malware and entities seeking to gain access to internal systems.' A Northeastern power provider said that it was 'under constant cyber attack from cyber criminals including malware and the general threat from the Internet...' A Midwestern power provider said that it was 'subject to ongoing malicious cyber and physical activity. For example, we see probes on our network to look for vulnerabilities in our systems and applications on a daily basis. Much of this activity is automated and dynamic in nature, able to adapt to what is discovered during its probing process." **Although these attacks occur with a great deal of frequency, none of the companies responding to the survey reported any sort of damage to the power grid as a result. Many of the attempted attacks were so minor in scope they were not reported to government authorities.**

#### 2. No doomsday cyberattack will take down the grid – damage is reversible

**Bobby Ghosh, 2009** (Bobby Ghosh, journalist for *Time* and the managing editor of the business news website *Quartz*. “How Vulnerable Is the Power Grid?” *Time*, [http://content.time.com/time/nation/article/0,8599,1891562,00.html](http://content.time.com/time/nation/article/0%2C8599%2C1891562%2C00.html). Accessed Nov 10 2016) ESG

As bad as all that may sound, there are several reasons not to panic about our power grid's vulnerability. •**No national power grid anywhere in the world has been brought down by a cyberattack.** And it's worth keeping in mind that most countries have much fewer defenses from cyberattacks than the U.S. "It's virtually impossible to bring down the entire North American grid," says Major General (Rtd) Dale Meyerrose, a cybersecurity expert who recently retired as chief information officer for the Director of National Intelligence. The electricity-distribution system is highly decentralized, and there's no central control system; at worst, cyberattackers may be able to damage sections of the grid. •**The most critical power users — the military, hospitals, the banking system, phone networks, Google's server farms — have multiple contingencies for uninterrupted power supply and backup generation. In the event of a cyberattack on the grid, they would be able to operate for long periods — days, weeks and, in some cases, indefinitely — without much difficulty.** •The power grid is far from perfect. On any given day, 500,000 Americans experience an outage, says Arshad Mansoor of the Electric Power Research Institute, which is funded by the utility industry. Why is this a good thing? Because it means **the grid deals with breakdowns all the time, and the industry knows how to fix them. The grid has built-in redundancies and manual overrides that allow for restoration of supply.** Mansoor is careful to point out that these are "not defenses against cyberattacks, but for dealing with the consequence of such attacks." •**The larger point is that in most cases, damage done to the power supply can be undone.** "In the banking system, if someone hacks the system and steals information about 500,000 credit cards, it's incredibly tough to undo that damage," says Mansoor. "But if a section of the power grid goes down, we start it up again."

#### 3. The greatest grid shutdowns are because of things like natural disasters, which we need IoT to detect

**Bobby Ghosh, 2009** (Bobby Ghosh, journalist for *Time* and the managing editor of the business news website *Quartz*. “How Vulnerable Is the Power Grid?” *Time*, [http://content.time.com/time/nation/article/0,8599,1891562,00.html](http://content.time.com/time/nation/article/0%2C8599%2C1891562%2C00.html). Accessed Nov 10 2016) ESG

•The larger point is that in most cases, damage done to the power supply can be undone. "In the banking system, if someone hacks the system and steals information about 500,000 credit cards, it's incredibly tough to undo that damage," says Mansoor. "But if a section of the power grid goes down, we start it up again." Of course, every power outage comes with a cost, not least to the economy. Mansoor would not discuss how long it would take to recover from a cyberattack — there are too many variables involved — but said **the longest delays in restoring power are typically caused not by technological glitches but by major acts of God, like hurricanes and earthquakes that destroy physical infrastructure.** (Read a TIME blog on China and hacking.)

#### 4. Smart grids make preventing hacks *easier*

**Silver Spring Networks, 2013** (Silver Spring Networks, leading networking platform and solutions provider for smart energy networks. 2013. “Smart Grid Security Myths vs. Reality,” *Silver Spring Networks*, <http://www.silverspringnet.com/pdfs/whitepapers/SilverSpring-Whitepaper-SmartGridSecurity-MythsReality.pdf>. Accessed Nov 10 2016) ESG

Myth #1: Nobody’s paying attention to security. A survey of utilities providers who have embarked on smart grid projects reveals that all of them are building security into their infrastructure. Likewise, **vendors of smart grid technology are implementing numerous security standards and mechanisms within their products, performing threat analysis and penetration tests on their systems and helping utility customers vet security architectures.** Standards bodies such as the National Institute of Standards and Technology (NIST), the North American Electric Reliability Corporation (NERC) and others are actively working with all stakeholders to define common industry security standards and testing procedures for smart grid networks. Myth #2: The smart grid makes it easy for hackers to cause widespread blackouts. The smart grid is designed to link together various devices for ease of management and operational control. **This architecture actually makes it easier to put a variety of checks, limits and restrictions at multiple points throughout the network.** For example, physical restrictions at the operations center can be combined with intelligence on every device in the field to check for proper authorization before any system-wide critical command, such as a remote disconnect, can be executed. **Smart grid operators can dramatically reduce the threat of a widespread blackout by taking a layered approach to network security that includes secure connectivity, perimeter security and identity and authorization services and by using dedicated network security hardware, software tools and effective security management policies.**

### AT: Big Data Bad

#### 1. Algorithmic systems can help reduce bias in employment

**Cecilia Munoz et al 2016** (Cecilia Munoz, director of the Domestic Policy Council, Megan Smith, US Chief Technology officer at the Office of Science and Technology Policy, and DJ Patil, Deputy Chief Technology Officer for Data Policy and Chief Data Scientist at the Office of Science and Technology Policy. May 2016. “Big Data: A Report of Algorithmic Systems, Opportunity, and Civil Rights,” *Executive Office of the President*, <https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf>. Accessed November 13th 2016. Page 14) ESG

**The Big Data Opportunity: Big data can be used to uncover or possibly reduce employment discrimination.** Just as with credit scoring, data analytics can be beneficial to the workplace in helping match people with the right jobs. **As discussed above, research has documented a “like me bias” or “affinity bias” in hiring; even well-intentioned hiring managers often choose candidates with whom they share characteristics. By contrast, algorithmically-driven processes have the potential to avoid individual biases and identify candidates who possess the skills that fit the particular job.**46 Companies can use data-driven approaches to find potential employees who otherwise might have been overlooked based on traditional educational or workplace-experience requirements. Data-analytics systems allow companies to objectively consider experiences and skill sets that have a proven correlation with success. By looking at the skills that have made previous employees successful, a human-resources data system can “pattern match” in order to recognize the characteristics the next generation of hires should have.47 When fairness, ethics, and opportunity are a core part of the original design, **large-scale data systems can help combat the implicit and explicit bias often seen in traditional hiring practices that can lead to problematic discrimination.** 48 Beyond hiring decisions, **properly deployed, advanced algorithmic systems present the possibility of tackling age-old employment discrimination challenges, such as the wage gap or occupational segregation.**

#### 2. Big Data can increase individual autonomy

Alex Bassi 2012 (Alex Bassi, He was the chair from 2007 until 2013 of the European Technology Platform on Smart Systems Integration "EPoSS" RFID / Internet of Things Working Group; currently, he is the co-chair of the Manufacturing WG. Rob van Kranenburg, He is co-founder of [bricolabs](http://bricolabs.net/%22%20%5Ct%20%22_blank) and the founder of [Council](http://blog.theitjobboard.co.uk/6-communities-internet-things-professionals/%22%20%5Ct%20%22_blank), author of several books on IoT. 2012. “IoT Challenges” from Communications in Global Commuting, Springer Open Journal. <http://muxjournal.springeropen.com/articles/10.1186/2192-1121-1-9> DOA: 10/17/16. P.4) ESM

IoT applications should be aimed to help the current institutions and public bodies to transform peacefully into a networked model of open data [6], direct feedback on where money goes, participatory budgeting models (say 25% for innovation in your street and neighborhood). IoT could be extremely relevant in making direct feedback visible in street and city furniture, and mobile applications. The internet of things can be a layer of data, open to all, through which individuals can decide for themselves what they are willing to pay for, get direct feedback from their voluntary donations, coordinate community spending that has a direct bearing to their needs through participatory budgeting [7,8]. What becomes clear in these challenges is that IoT cannot be managed with the current policy tools and research programs. They are too slow and too instrumental. There is too little sense of urgency; of the larger picture of Climate Change that should be the one issue the main umbrella research questions are parsed to, and of the upcoming breakdown in managing societal drivers in an inclusive way.

#### 3. Big Data can help make policing more accurate and more transparent

**Cecilia Munoz et al 2016** (Cecilia Munoz, director of the Domestic Policy Council, Megan Smith, US Chief Technology officer at the Office of Science and Technology Policy, and DJ Patil, Deputy Chief Technology Officer for Data Policy and Chief Data Scientist at the Office of Science and Technology Policy. May 2016. “Big Data: A Report of Algorithmic Systems, Opportunity, and Civil Rights,” *Executive Office of the President*, <https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf>. Accessed November 13th 2016. Page 19-20) ESG

The Big Data Opportunity: **Data and algorithms can potentially help law enforcement become more transparent, effective, and efficient.** Law enforcement agencies have long attempted to identify patterns in criminal activity in order to allocate scarce resources more efficiently. New technologies are replacing manual techniques, and many police departments now use sophisticated computer modeling systems to refine their understanding of crime hot spots, linking offense data to patterns in temperature, time of day, proximity to other structures and facilities, and other variables. **The President’s Task Force on 21st Century Policing recommended, among many other steps, that law enforcement agencies adopt model policies and best practices for technology-based engagement that increases community trust and access; work toward national standards on the issue of technology’s impact on privacy concerns; and develop best practices** that can be adopted by state legislative bodies to govern the acquisition, use, retention, and dissemination of auditory, visual, and biometric data by law enforcement.66 Since the Task Force released its recommendations, the White House and the Department of Justice have been engaged in several initiatives to ensure that the report’s recommendations are put into practice across the United States. As part of these efforts, the White House launched the Police Data Initiative to make policing data more transparent and improve community trust.67 More than 50 police departments throughout the nation have joined in this work to realize the benefits of better technology. Commitments from participating jurisdictions include: increased use of open policing data to build community trust and increase departmental transparency, and use of data to more effectively identify policies that could be improved or officers who may contribute to adverse public interactions so they can be linked with effective training and interventions.68 **Consistent with these goals, several police departments in the United States have developed and deployed “early warning systems” to identify officers who may benefit from additional training, resources, or counseling to prevent excessive uses of force, citizen complaints and other problems.** 69 Using de-identified police data, as well as contextual data about local crime and demographics, **these systems are designed to detect the factors most indicative of future problems by attempting to determine behavioral patterns that predict a higher risk of future adverse incidents.** Detecting these patterns opens new opportunities to develop targeted interventions for officers to protect their safety and improve police/community interactions. Separately, some of the newest analytical modeling techniques, often called “predictive policing,” might provide greater precision in predicting locations and times at which criminal activity is likely to occur. Research demonstrates that a neighborhood that has recently been victimized by one or more burglaries is likely to be targeted for additional property crimes in the coming days. An analytical method known as “near-repeat modeling” attempts to predict crimes based on this insight.70 Similarly, a technique known as “risk terrain modeling” can identify specific locations where criminal activity often clusters, such as bars, motels or convenience stores, and can predict the specific social and physical factors that attract would be offenders and create conditions ripe for criminal activity.71 Current Los Angeles Police Department (LAPD) Chief of Police, Charlie Beck, described predictive policing as enabling “directed, information-based patrol; rapid response supported by fact-based prepositioning of assets; and proactive, intelligence-based tactics, strategy, and policy.”72 In some instances these systems have shown significant promise. In experiments conducted by the LAPD’s Foothill Division in which large sets of policing data were analyzed to predict occurrences of crime, the Division experienced a larger reduction in reported crime than any other division in the Department.73

### AT: Save the Bees!!!

#### 1. The beez are back

**Matt Miller, 2016** (Matt Miller, veterinary student and science writer for *Slate*. July 29th 2016. “The Bees Are All Right,” *Slate*, <http://www.slate.com/articles/health_and_science/science/2016/07/colony_collapse_disorder_is_no_longer_the_existential_threat_to_honeybees.html>. Accessed Nov 19 2016) ESG

**The strange thing is that no one knows exactly how the interaction of bad pesticides and this parasite caused bee colonies to collapse.** Some researchers have argued that the pesticides make the queen more susceptible to varroa mite, which kills her reproductive capabilities and causes other members of the hive to give up and depart for greener pastures, so to speak. Others think it’s that the neonicotinoids cause a disruption in the homing mechanisms of the honeybees that prevents them from navigating back home, though it’s unclear how the mites play a role. In both cases, the result is the same: an empty hive. “CCD was a real problem, probably six or seven years ago,” says Jeff Pettis, an entomologist whose research played a major role in uncovering the causes of CCD. He adds that **in the past three to five years, though, researchers** in his field **have as not seen much CCD and that globally honeybee populations are not in decline.** The reasons for this apparently miraculous departure from the fast-track toward extinction are not hard to understand, now that research has borne out the causes. First, both the U.S. and several European countries have passed regulations that restricts the use of pesticides and fungicides that are suspected to have played a role in CCD to begin with. The second reason there’s no longer an immediate threat of extinction is that **bees aren’t, say, giant pandas, an animal that is actually, seriously endangered. That is to say, bees can recover their population numbers reasonably quickly.** Compared with the once-a-year ovulatory habits of pandas, **queen honeybees regularly lay 1,500 eggs per day, and if the conditions call for it, can up that figure to as many as 2,000 eggs per day or more.** Even if honeybee keepers report losing as much 30 to 45 percent of their bees in a single year, this doesn’t actually mean the honeybee population will decline by that much. The beekeepers’ response will be to simply leverage the queens’ enormous reproductive abilities, which will quickly recoup those losses. So even though bees were disappearing in alarming ways and at alarming rates, **their population never actually saw a significant decline.** The number of honeybee colonies peaked in 1989, at 3.5 million colonies; in 2008, two years after CCD was first characterized, that number dipped to 2.4 million, the worst year for honeybee populations in recorded history. **Since their lowest point, honeybee populations in the U.S. have climbed at a modest pace and now stand at 2.7 million colonies.**

#### 2. Turn – a large problem for bees is the loss of land due to climate change

**Justin Worland 2015** (Justin Worland, writer for Time Magazine. July 9, 2015. DOA: November 12, 2016. “Bees Are Losing Their Habitat Because of Climate Change,” Time Magazine. <http://time.com/3951339/bees-climate-change/>) EL

As if pesticides, disease and habitat loss were not enough, there’s more bad news for bees. **Changing temperature and weather conditions due to climate change has restricted the area where bees can survive, and the pollinators have struggled to adapt,** according to new [research](http://www.sciencemag.org/lookup/doi/10.1126/science.aaa7031%22%20%5Ct%20%22_blank) published in the journal Science. “They just aren’t colonizing new areas and establishing new populations fast enough to track rapid human-caused climate change,” said study author Jeremy Kerr, a professor at the University of Ottawa, on a call for journalists. “Impacts are large and they are underway. They are not just something to worry about at some vague, future time.” For the study, **researchers looked at 110 years of data on 67 bumblebee species to track their movements over time. Activity between 1901 and 1974 was compared to movement in recent decades when climate change accelerated. In the northern end of their range, bees have failed to migrate closer to the North pole. In the southern end, many populations have died. Altogether, bees have lost a range of up to nearly 200 miles in both North America and Europe**. The study, which evaluated land use changes and pesticide application in addition to weather conditions, attributed the drop to climate change. For the study, researchers looked at 110 years of data on 67 bumblebee species to track their movements over time. Activity between 1901 and 1974 was compared to movement in recent decades when climate change accelerated. In the northern end of their range, bees have failed to migrate closer to the North pole. In the southern end, many populations have died. **Altogether, bees have lost a range of up to nearly 200 miles in both North America and Europe. The study, which evaluated land use changes and pesticide application in addition to weather conditions, attributed the drop to climate change.**

### AT: Unaffordability

#### 1. Earthquake early warning systems are affordable

**Richard Armitano 2016** (Richard Armitano, PhD in Digital Signal Processing from Georgia Tech and a B.S. in Electrical Engineering from Stanford University and former research scientist at Hewlett-Packard Labs. “IoT Provides Affordable Earthquake Early Warning to Communities,” *The Huffington Post*, <http://www.huffingtonpost.com/robert-armitano/iot-provides-affordable-e_b_10055446.html>. November 15th 2016) ESG

Earthquakes come without warning, making them one of the most feared natural disaster. Startups like Zizmos are working on early-warning systems using IoT (Internet of Things) sensors. Earthquake detection is provided by interconnecting multiple seismic sensors to a central server. The system works by detecting motion close to the earthquake epicenter and transmitting a warning alert to users further away from the epicenter. The system requires a large number of sensors to cover earthquake prone areas. **Sensor costs have significantly decreased over the last decade through advances in smart phone and wearable technology, making an earthquake early-warning system affordable.** Japan has experienced many large seismic events in its history and takes earthquake hazards seriously, imposing strict building codes and investing in disaster response personnel. Even then, extensive damage and loss of life occurs with every major Japanese earthquake. After the catastrophic 7.3 magnitude Kyoto earthquake in 1995 with a death toll of 6,434, Japan’s government created additional safeguards for its citizens in the form of seismic early warning systems. **An earthquake early warning system provides safeguards for industries and people. Industrial activities can be halted before the onset of an earthquake allowing workers to secure sensitive equipment. People can take cover in safe areas preceding an earthquake to help reduce injuries and loss of life.**

#### 2. You don’t need water IoT in every field. There are effective ways to scale the price of precision agriculture

USDA 2003 (The United States Department of Agriculture provides leadership on food, agriculture, natural resources, rural development, nutrition, and related issues based on public policy, the best available science, and effective management. March 2003. “Affordable Opportunities For Precision Farming,” USDA. <http://open-furrow.soil.ncsu.edu/Documents/On-point/Precision_Farming.pdf> PAGE: 10. DOA 11/19/16) CDY

Much information about spatial variability on a farm can be determined and managed by directly observing crop **A less expensive method of soil sampling for spatial variability is directed soil sampling. Directed soil sampling focuses individual samples in areas that are likely to have different characteristics. For example, areas in which yield is consistently higher or lower than the rest of the field, areas with minor landscape fluctuations, and areas with distinctly different soil types may warrant separate soil samples. Over time, these samples could help the farmer establish management zones within the field.** Each management zone must be tested or monitored separately. When sampling an area, producers must be aware of variation within the area they are testing to avoid systematic bias. For example, always sampling in the bottom of the furrow can lead to a result different from sampling the entire area between rows. Farmers avoid this problem by collecting soil from a variety of positions and mixing it well before subsampling and sending it for analysis. Soil pH, organic matter, and phosphorus often vary by depth, so the soil must be sampled to exactly the desired depth to avoid misleading results.

#### 3. High costs in the developing world can be solved

**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.**

### AT: E-Waste and Stuff

#### **1. IoT procedures could be changed so that IoT has a low carbon footprint**

Phillip Tracy 2016 ([Phillip Tracy](http://www.rcrwireless.com/author/ptracy), reports on Industrial IoT and 5g. OCTOBER 4, 2016 “Keeping the IoT green by reducing e-waste” from RCR Wireless News. <http://www.rcrwireless.com/20161004/telco-cloud/green-iot-e-waste-tag31-tag99> DOA: 11/17/16) ESM

New technologies are fighting an uphill battle to reduce the environmental decay from century-old processes that are both inefficient and wasteful. The “internet of things” has the potential to reduce emissions from those processes and create a truly green earth. But while green use cases like water monitoring, smart grid and metering are all well known within enterprise IoT, the concern for the e-waste impact of IoT itself is less of a focus. We have all read the projections of tens of billions of connected devices in the next few years, but how do we account for the production of those devices that require connectivity and energy? What happens when a device fails, or needs an update that cannot be done over the air? IoT can do a lot for our environment, but at the expense of a potentially significant increase in [e-waste](https://en.wikipedia.org/wiki/Electronic_waste) and energy usage. This is why “green IoT” is not just how the internet of things is helping reduce the greenhouse effect within other industries, but also reducing the effect that IoT itself could have on the environment. According to an Institute of Electrical and Electronics Engineers [report](http://www.ieeeexplore.ws/xpls/icp.jsp?arnumber=7317502) titled Green Internet of Things for Smart World, green IoT can be defined as: ‘‘The energy efﬁcient procedures (hardware or software) adopted by IoT either to facilitate reducing the greenhouse effect of existing applications and services or to reduce the impact of greenhouse effect of IoT itself. In the earlier case, the use of IoT will help reduce the greenhouse effect, whereas in the later case further optimization of IoT greenhouse footprint will be taken care. The entire life cycle of green IoT should focus on green design, green production, green utilization and ﬁnally green disposal/recycling to have no or very small impact on the environment.’’

#### 2. **E-waste can be reduced with product innovation and recycling products**

Chad Lander 2011 (Chad Lander, Senior Vice President - Distribution Channel Strategy and Development at eRecyclingCorps. Oct 28th, 2011 “E-Waste – Reducing Its Impact through Innovation” from Triple Pundit. <http://www.triplepundit.com/2011/10/waste-reducing-impact-innovation/> DOA: 11/18/16) ESM

We are also thinking of new ways to involve customers in e-waste solutions. Through our Reverse Logistics process, we look first for opportunities to service and remanufacture mobile devices to get them in proper working order. Additionally, our customers typically receive certified, pre-owned devices as replacements in our stores, which is a more cost-effective and environmentally responsible option. Pre-owned certified devices are also available for purchase on Sprint.com at a fraction of the cost of a new device. Both efforts help save customers money and reduce e-waste. Companies can also grow access to refurbished products and reduce e-waste by finding new ways to collect e-waste. One company that has made great strides with its comprehensive approach to managing the lifecycle of computers is Dell. The company offers easy and convenient ways to drop-off products at more than 2,000 Goodwill locations across the U.S. Additionally, with its TechForward Buyback Plan, Dell offers customers instant cash back when they upgrade to a new computer and return their old model. Computers gathered through these two programs are either remanufactured and reused or disposed of responsibly by certified recyclers. Through product innovation, working with suppliers throughout the supply chain, and using savvy strategies for engaging customers in reuse and recycling, electronics companies can significantly reduce the size of America’s growing e-waste footprint and mitigate potential risks it poses to the environment and the health of our communities.

#### 3. **The EPA is already solving the problem of E-waste by improving waste management all over the world**

EPA 2015 (EPA, Environmental Protection Agency Last updated: December 11, 2015 “Cleaning Up Electronic Waste (E-Waste)” from EPA. <https://www.epa.gov/international-cooperation/cleaning-electronic-waste-e-waste> DOA: 11/18/16) ESM

EPA efforts support the United States government's [National Strategy for Electronics Stewardship](https://www.epa.gov/smm-electronics/national-strategy-electronics-stewardship-nses), which details the federal government’s plan to enhance the management of electronics throughout the product lifecycle. EPA collaborates with the United Nations University - Solving the E-waste Problem Initiative (StEP) to jointly address the e-waste problem in developing countries. EPA and StEP signed a cooperative agreement on this topic in November 2010. EPA and StEP are working collaboratively on tracking global flows of e-waste, strengthening Ethiopia's efforts to manage e-waste. EPA is a founding member of StEP and serves on the StEP Steering Committee. EPA also works bilaterally with governments and environmental officials around the world on e-waste management. [EPA and China’s Ministry of Environmental Protection](https://www.epa.gov/international-cooperation/epa-collaboration-china) initiated cooperation on this issue in 2010. In addition, EPA and Environmental Protection Administration Taiwan (EPAT) coordinate the [International E-Waste Management Network (IEMN)](https://www.epa.gov/international-cooperation/international-e-waste-management-network-iemn), which has brought together environmental officials from Asia, Latin America, the Caribbean, Africa, and North America to exchange best practices on e-waste management since 2011.

### AT: Surveillance

#### 1. Surveillance fails—the data just isn’t useful to law enforcement

**Marshall Erwin 2016** (Marshall Erwin, senior staff analyst; 4/17/16; "The Internet-of-Things-That-Are-Marginally-Useful-for-Surveillance" The Cipher Brief; DOA: 11/12/16; <https://www.thecipherbrief.com/article/techcyber/internet-things-are-marginally-useful-surveillance-1092>) AM

**The Internet-of-Things** has for years promised to usher in a new wave of innovation. It has sometimes been called the Internet-of-Everything or Internet 3.0—grand language illustrating its potential. That potential would also seem to offer new opportunities for law enforcement and intelligence services. But the promise has thus far not materialized. I prefer, somewhat glibly, to use my own term for this wave of technological change: the Internet-of-Things-That-Are-Marginally-Useful-for-Surveillance (IOTTAMUFS). I use this term because the IOTTAMUFS **is not going to be the boon to law enforcement and intelligence services that [some suggest](https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf%22%20%5Ct%20%22_blank).** Here is why. The IOTTAMUFS presents two fundamental privacy and security challenges. First the privacy problem: consumers have no ability to understand the way in which IOTTAMUFS devices will collect and use data about them. As a result, they can’t provide meaningful consent to the collection. This problem already exists across the Internet today, but when consumers visit a website or use their iPhone, many at least have some idea that data collection is occurring in the background. That isn’t the case when everyday devices, like refrigerators or thermostats, collect data. Second, the security problem: for these everyday devices, it is going to be difficult to update or patch software or even to build strong security in the first place. As a result, many are going to be extremely vulnerable to compromise. A consumer privacy problem coupled with a product security problem are the two most fundamental ingredients for a surveillance opportunity, whether that surveillance is carried out by an intelligence agency, law enforcement, or a malicious hacker. And as privacy and security issues go, these two problems are massive. Industry isn’t anywhere close to figuring out how to solve them. But **much of the data that is going to be collected by these everyday devices—and potentially going to be available for surveillance purposes—just isn’t going to be that useful. It is low value data. The data likely to be exposed isn’t often going to be data that intelligence and law enforcement agencies actually want.** I agree with the general argument made in the recent encryption debate that law enforcement has access to huge amounts of data today that can allow it to compensate for a lose of access due to encryption. But this argument rests on an assumption that isn’t always true – that the data law enforcement is gaining access to is as valuable for investigative purposes as the access it is losing. In some cases, such as the growing volume of geolocation data available, the argument holds up. In other cases, such as the IOTTAMUFS, it might not. For example, consider data collected and used by the adtech industry. The Internet has brought a revolution to the advertising industry that is as consequential as the rise of the iPhone. Ad tech companies now collect vast amounts of data about Internet users that can be used to build consumer profiles and target advertising. The scope of this collection is staggering. However, **despite the quantities of that data collected, this revolution in technology has not been nearly as consequential to law enforcement.** The data in question simply isn’t that valuable outside of the context in which it is collected and used. The same is going to be true for much of the data collected by IOTTAMUFS devices. **The data from your thermostat or refrigerator just isn’t going to be as valuable as the data on your phone**. What does this mean for the privacy and security challenges mentioned earlier? It means that the **surveillance opportunities** created by these two fundamental problems **are only going to be useful in a small number of cases, involving extremely motivated attackers targeting key individuals.** It is only in those cases where someone will invest the time and effort to exploit vulnerabilities in IOTTAMUFS devices and figure out how to derive some value out of large quantities of mostly useless data. **These new devices will create opportunities to collect information about heads of state but won’t be as helpful when it comes to standard criminals or lower level intelligence targets.** This is consistent with the general tend that we’ve seen in recent years and that is likely to continue: highly targeted surveillance that takes longer to execute will become easier even while quick, more broadly applicable surveillance becomes harder. Simply put, the attack surface for the products and systems we use has broadened and diversified. And while this provides an abundance of niche opportunities, it also means that there will be fewer simple surveillance solutions in the future.

#### 2. Privacy is *not* an absolute right – personal safety trumps

**Kenneth Himma, 2007** (Kenneth Einar Himma, associate professor philosophy at Seattle Pacific University. 2007. “Privacy Versus Security: Why Privacy is Not an Absolute Value or Right,” *San Diego Law Review*, http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=994458. Accessed 9/4/2016. Page 878) ESG

**From an intuitive standpoint, the idea that the right to privacy is an absolute right seems utterly implausible. Intuitively, it seems clear that there are other rights that are so much more important that they easily trump privacy rights in the event of a conflict.** For example, if a psychologist knows that a patient is highly likely to commit a murder, then it is, at the very least, morally permissible to disclose that information about the patient in order to prevent the crime—regardless of whether such information would otherwise be protected by privacy rights. Intuitively**, it seems clear that life is more important from the standpoint of morality than any of the interests protected by a moral right to privacy.** Still one often hears—primarily from academics in information schools and library schools, especially in connection with the controversy regarding the USA PATRIOT Act—the claim that privacy should never be sacrificed for security, implicitly denying what I take to be the underlying rationale for the PATRIOT Act. This also seems counterintuitive because it does not seem unreasonable to believe we have a moral right to security that includes the right to life. Although this right to security is broader than the right to life, the fact that security interests include our interests in our lives implies that the right to privacy trumps even the right to life—something that seems quite implausible from an intuitive point of view. If I have to give up the most private piece of information about myself to save my life or protect myself from either grievous bodily injury or financial ruin, I would gladly do so without hesitation. There are many things I do not want you to know about me, but should you make a credible threat to my life, bodily integrity, financial security, or health, and then hook me up to a lie detector machine, I will truthfully answer any question you ask about me. **I value my privacy a lot, but I value my life, bodily integrity, and financial security much more than any of the interests protected by the right to privacy.**

#### 3. Privacy loss is inevitable in the technological age – the regular Internet kills it regardless

**Ron Iphofen, 2016** (Ron Iphofen, adviser in research ethics to the European Commission. April 28th 2016. “Safety is more important than privacy,” *Times High Education*, <https://www.timeshighereducation.com/features/safety-is-more-important-than-privacy>. Accessed September 9th 2016) ESG

**It is not that I don’t value privacy; it is rather that I do not expect that large aspects of my life can ever be considered private again. If privacy is not exactly “dead”, it is certainly staggering about uncertainly. There have been a range of revelations over recent years vindicating the view that privacy cannot be ensured in the modern, technological age. These include the newspaper phone-hacking scandal; a bug in Facebook’s data archive exposing the personal details of about 6 million people**; the “mistaken” collection of data by Google’s Street View equipment in 30 countries (including complete email messages, logging-in details and medical listings); and, of course, Edward Snowden’s whistleblowing of the automated interrogation of international communications by US and UK intelligence agencies. Some commentators, such as Kelvin Wade, have even announced that privacy is “a 20th-century concept”. And surveillance from all sources has grown rapidly in line with technological developments and the assumed rise in threats to public safety.

### AT: Drones are Bad

#### 1. Drone strikes kill significantly fewer people than conventional warfare

**William Saletan, 2015** (William Saletan, intelligence writer for *Slate Magazine.* April 24th 2015. “Don’t Blame Drones,” *Slate Magazine*, <http://www.slate.com/articles/news_and_politics/foreigners/2015/04/u_s_drone_strikes_civilian_casualties_would_be_much_higher_without_them.html>. Accessed Nov 19 2016) ESG

The outrage is understandable. But these two deaths, tragic as they are, don’t change the fundamental truth: **For civilians, drones are the safest form of war in modern history.** As I’ve documented before, **they’re more discriminating and more accurate. If you want to minimize civilian casualties, getting rid of drones—and steering warfare back to bombing and shelling—is the worst thing you could do.** Look at the record in Pakistan. The harshest tally of drone strikes, maintained by the Bureau of Investigative Journalism, says drones have killed 2,449 to 3,949 people there, including 423 to 962 civilians. If you work with the low-end figures, that’s a civilian casualty rate of 17 percent. If you use the high-end figures, it’s 24 percent. In Yemen, the bureau counts 436 to 646 deaths by drone, of whom 65 to 96 were civilians. That’s a rate of 15 percent. If you factor in other incidents classified as possible but unconfirmed drone strikes, the rate in Yemen drops to somewhere between 8 percent and 14 percent. **The New America Foundation** keeps a different tally. Its figures **imply a civilian casualty rate of 8 percent to 12 percent in Pakistan and 8 percent to 9 percent in Yemen.** A third count, maintained by the Long War Journal, indicates a 5 percent civilian casualty rate in Pakistan (once Weinstein and Lo Porto are added to the tally) and 16 percent in Yemen. Compare those numbers with any other method of warfare. **Start with an apples-to-apples comparison: the Bureau of Investigative Journalism’s analysis of “other covert operations” in Yemen.** According to BIJ’s methodology, this category consists of nondrone attacks by U.S. forces, “including airstrikes, missile attacks and ground operations.” **BIJ counts** 68 to 99 civilian deaths in these operations, among 156 to 365 total casualties. That’s **a civilian casualty rate of 27 percent to 44 percent: three times worse than drone strikes in the same country. Or look at the bureau’s data from Somalia. For drones, the BIJ counts 23 to 105 casualties, of whom zero to five were civilian. For other covert operations, the BIJ counts 40 to 141 casualties, of whom seven to 47 were civilian. If you go with the low-end numbers, drones have a perfect record in Somalia. If you go with the high-end numbers, drones are seven times safer than the alternatives.**

#### 2. Drones are good they save lives

Juliet Eysenck 2016 (Juliet Eysenck, writer for the telagraph; May 25 2016; "How Drones are changing our lives: the good, the bad and the lazy"; DOA: 11/11/16; <http://www.telegraph.co.uk/technology/2016/05/23/how-drone-technology-is-changing-our-lives-the-good-the-bad-and/>) AM

**Drones have the potential to transform the world for the better.** In the UK, the **emergency services have started to use them to help people in danger,** while the defence industry is exploring how drones can improve security. **Around the world, wildlife conservationists are embracing the technology to monitor animals and any potential threats against them** by using drones. European **emergency services are being trained on how to use consumer drones in rescue operations and emergencies, including chemical spills, car accidents and widespread fires**. Ireland's Donegal Mountain Rescue Team has been using advanced drone software to help coordinate search and rescue missions in remote areas, while the Greater Copenhagen Fire Department in Denmark will be taught how to use drones to combat fires, chemical accidents and pile ups in both urban and over-water conditions. Marine biologists from the Leatherback Trust, a non-profit organisation, are using drones to monitor sea turtles, in a bid to uncover secrets about their behaviour in the open ocean. Tracking them by swimming out alongside turtles, or even using a boat, is a tricky task, but drones allow scientists to follow the turtles over long distances without disturbing them. Dr Nathan Robinson, field director at the Leatherback Trust, said: "A lot of our work involves trying to find out where sea turtles are nesting. It usually means walking up and down beaches for long periods of time. Instead, you can send out a drone and look at the footage and work out where the nests are." In South Africa, unmanned drones have been deployed to track suspected poachers to help tackle the number of endangered rhino deaths. The small, lightweight drones can be launched by hand in minutes and fly over a range of five miles for up to 90 minutes. Fitted with high-resolution infrared cameras, they can pick out elephants, rhinos and lions as well as anyone that might be tracking them.

#### 3. It helps farmers who tend to be some of the most underprivileged people in the world

Juliet Eysenck 2016 (Juliet Eysenck, writer for the telagraph; May 25 2016; "How Drones are changing our lives: the good, the bad and the lazy"; DOA: 11/11/16; <http://www.telegraph.co.uk/technology/2016/05/23/how-drone-technology-is-changing-our-lives-the-good-the-bad-and/>) AM

A report by PwC claims that **American businesses could make savings of $127billion by adopting drone-powered solutions. The industry with the most to gain is infrastructure, where drones could be employed to collect data in remote areas, such as carrying out inspections on wind turbines, tunnels or bridges. In agriculture, drones could analyse the soil to determine when fields need to be sprayed and whether they are lacking in certain nutrients. From improving safety to cutting costs, there are many benefits** to be gained from using drones. Man versus machine? The choice is yours.

### AT: Data Centralization

#### 1. Europe already wanted to create localized data

The Economist 13 (The Economist, magazine that covers a variety of international issues, November 18th 2013, “Data Protectionism,” <http://www.economist.com/news/21589110-global-computing-cloud-geography-will-matter-more-data-protectionism>, DoA 11/19/16) CJV

It is anyway not seamlessly global, because of technical and regulatory constraints. Some companies, such as makers of online games, want data to travel only short distances, to save every millisecond (bits cannot go faster than light). Banks and health-care providers are often told that they must keep data within national or European borders. More generally, customers of big providers of remote computing power may already insist that they be served only by data centres in a specific region. Now politics has been added to physics and bur-eaucracy. European politicians, in particular, have long cast envious glances at American dominance of information technology. Even before the Snowden affair, they had hoped to build national or regional cloud capacity. In France two companies, Cloudwatt and Numergy, both established in 2012 with state backing, promise customers that their data will be stored on French soil.

#### 2. American surveillance is the actual link

The Economist 13 (The Economist, magazine that covers a variety of international issues, November 18th 2013, “Data Protectionism,” <http://www.economist.com/news/21589110-global-computing-cloud-geography-will-matter-more-data-protectionism>, DoA 11/19/16) CJV

Worries that the Americans may be snooping has given extra urgency to the arguments for a European cloud. “Europe’s strategic interest is served by having its own capacity to deliver secure cloud-computing services to citizens and businesses,” said Neelie Kroes, the European commissioner responsible for the EU’s “digital agenda”, in September 2013. “Europe should not be at the mercy of cloud-computing providers outside Europe.” In July 2013, in the wake of the Snowden affair, German data-protection authorities at both federal and state levels stopped issuing approvals for the transfer of personal data outside the European Union. In September they recommended a review of “whether routing of telecommunications connections can take place only over networks within the eu”. The affair also gave more urgency to a long-planned overhaul of the EU’s data-protection law—although in October ministers pushed the deadline for this back from 2014 to 2015.

#### 3. Not just in Europe, but all over the world, Brazil as an example

The Economist 13 (The Economist, magazine that covers a variety of international issues, November 18th 2013, “Data Protectionism,” <http://www.economist.com/news/21589110-global-computing-cloud-geography-will-matter-more-data-protectionism>, DoA 11/19/16) CJV

Such concerns are not confined to Europe. Allegations of American snooping have prompted Brazil’s president, Dilma Rousseff, to propose measures to insulate the country’s internet. Whether all this will benefit non-American cloud companies much is hard to say. American firms are a long way ahead. It could just be that American companies step up their provision of capacity outside the United States. Still, there are some signs that customers as well as officials are uneasy. Some have reported cancelling deals with American cloud providers. A Swiss company has reported a marked post-Snowden increase in enquiries for data storage. The Information Technology & Innovation Foundation, a think-tank in Washington, believes that the Snowden affair could cost the American cloud industry between $21.5 billion and $35 billion in 2014-16. In the worst case, it says, American companies’ share of the market outside the United States would drop from 85% to 55%. The cloud has hitherto been largely American. It will soon have a more local flavour.

#### 4. You don’t gotta

#### 5. Even if it *was* unique, centralized data can be good

**Target Marketing 2016** (Target Marketing, a promotional marketing agency – this is from their magazine publication. March 14th 2016. “The One: 5 Benefits of Committing to a Single, Centralized Database,” *TargetMarketing*, <http://www.targetmarketingmag.com/partner/the-one-5-benefits-of-committing-to-a-single-centralized-database/>. Accessed Nov 19 2016) ESG

**1. It Reduces Bad Data Bad data costs money.** It costs money to acquire, money to store and (mis)manage, and money that you miss out on when it loses sales. A Gartner survey found that companies know bad data costs them money, an average of $14 million from the companies they surveyed. A separate study by LeadJen found that bad data costs companies $20,000 per sales rep per year. Experian says 75 percent of companies are wasting 15 percent of their revenue due to poor data quality. And there’s a lot more data that says the same thing where they came from. **A lot of data inconsistency is caused by maintaining information in parallel databases, transferring data from department to department, and not having a single point of responsibility for keeping it all clean and up to date. Bringing all of your data into a centralized system is essential to solving this problem. 2. Saves Time and Money** This seems obvious, but it’s really a top reason to get your data into one central database. It may take a higher level of expertise to manage a centralized marketing database, but **it takes a lot less personnel time than having multiple departments manage separate databases in separate repositories or Excel files.** It’s not just about wasted time or effort, there is work and analysis that simply does not happen with the data being managed by different folks in different departments across your company. **3. Enables Cross-Silo Tracking and Messaging Cross-sell, up-sell, opportunistic sales based on the customer’s needs …** none of these things are possible if data doesn’t travels from lead generation through nurturing, sale, post-sale and customer service. **The best way to do that is to have one database that all of those departments can access, one record all of those departments can build upon.** Think beyond marketing for a moment. Think of how customer service works with sales. If a customer calls in to customer service with a problem, and sales is going to call on that customer again in the future, details of that interaction should be in the same database the salesperson is using. The salesperson can at least mention the service call to break the ice, and may be able to makes cross-sell or up-sell offers based on the experience. That’s why research from Experian Data Quality Services found that the top two reasons companies reported for keeping high quality data were “increase efficiency” and “enhancement of customer/client satisfaction.” **4. More Accurate and Insightful Analytics** Want to know how lead source and nurturing steps impact the post-purchase customer experience and lifetime value? You’re not alone; **analytics and reporting are often at the top of marketer’s list of reasons for purchasing marketing technology. Any technology that enables that will require a centralized database (or provide one). 5. Easier to Prove ROI and Get Executive Buy-in** This is related to the point above, but the consequences of this particular shortcoming are far ranging. **Marketers have long struggled to be recognized as a revenue center by the C-suite. And it doesn’t help when the boss asks a quantitative question, and your best answer is to stall for time because it’ll take time to pull that information together from several different systems.** Having a central database is the first step to embracing all the technology and opportunity available to marketers today. Don’t be left behind.

### AT: Rebound

#### 1. Rebound effect doesn’t match up with data

Shakeb Afsah 2012 (Shakeb Afsah is the Director of Policy Analysis at the CO2 Scorecard Group and a former environmental economist at the World Bank’s Development Research Group. January 11, 2012. “Energy Efficiency is for Real, Energy Rebound a Distraction,” CO2 Scorecard. <http://co2scorecard.org/Content/uploads/Energy_Efficiency_is_for_Real_CO2_Scorecard_Research_Jan_11_12.pdf> Page:1 DOA: 11/19/16) CDY

Energy efficiency is an over-rated policy tool when it comes to cutting energy use and CO2 emissions— that’s **the basic message** promoted by the US think tank the Breakthrough Institute (BTI), and amplified in major news outlets like the New Yorker and the New York Times. Their logic is **that every action to conserve energy through efficient use leads to an opposite reaction to consume more energy—a “rebound” mechanism**, which, according to the BTI, can negate as much as 60-100% of saved energy, and in some cases can backfire to increase net energy consumption. In this research note we refute this policy message and show that the BTI, as well as its champions in the media, have overplayed their hand, supporting their case with anecdotes and analysis that don’t measure up against theory and data. Our fact-checking revealed that empirical estimates of energy rebound cited by the BTI **are over-estimated or wrong, and they contradict the technological reality of energy efficiency gains observed in many industrial sectors.** We provide new statistical evidence to show that energy efficiency policies and programs can reliably cut energy use—a finding that is consistent with the policy stance of leading experts and organizations like the US Energy Information Agency (EIA) and the World Bank. Additionally, we take our policy message one step further—by using new insights from the emerging multi-disciplinary literature on “energy efficiency gap”, we recommend that the world needs more energy efficiency policies and programs to cut greenhouse gases—not less as implied by the BTI and its cohorts in the media.

#### 2. It’s dangerous to accept the rhetoric of the rebound effect, it’s an excuse for inaction

Shakeb Afsah 2012 (Shakeb Afsah is the Director of Policy Analysis at the CO2 Scorecard Group and a former environmental economist at the World Bank’s Development Research Group. January 11, 2012. “Energy Efficiency is for Real, Energy Rebound a Distraction,” CO2 Scorecard. <http://co2scorecard.org/Content/uploads/Energy_Efficiency_is_for_Real_CO2_Scorecard_Research_Jan_11_12.pdf> Page:2 DOA: 11/19/16) CDY

The Rebound Effect deserves to be taken seriously, not just because there is an undeniable trend in global energy use to show that humanity has never successfully decreased energy use, but also because **the idea is extremely powerful for those seeking reasons to disregard efficiency – whether in support of an alternate climate initiatives or in opposition to climate change in general. If the Rebound Effect can take back as much as 60-100% of energy savings,** as implied by the narrative sketched by the BTI, **there is no way that the world can achieve the projected reductions in GHG emissions from energy efficient approaches. In essence, the Rebound Effect has the power to derail climate policy as a whole, simply by calling into question energy efficiency.** Recognizing this seriousness, we began a detailed investigation of the economics and the science behind the Rebound Effect. We examined the sources of energy Rebound resurgence, finding that the current polemic against energy efficiency is largely fuelled by a study that is neither published nor peer-reviewed. We review the literature on energy Rebound at household and production-sector levels and identify weaknesses in both the source data and the methodology employed by Rebound’s proponents. We not only disprove the claims of Reboundistas but through our original statistical analysis we reaffirm that energy efficiency policies indeed reduce per capita energy use.

#### 3. When Canada increased efficiency, they saw a downward trend in emissions

Shakeb Afsah 2012 (Shakeb Afsah is the Director of Policy Analysis at the CO2 Scorecard Group and a former environmental economist at the World Bank’s Development Research Group. January 11, 2012. “Energy Efficiency is for Real, Energy Rebound a Distraction,” CO2 Scorecard. <http://co2scorecard.org/Content/uploads/Energy_Efficiency_is_for_Real_CO2_Scorecard_Research_Jan_11_12.pdf> Page:4 DOA: 11/19/16) CDY

**We found the same pattern in Canada, where residential energy efficiency programs have been in use since 1982. As shown in Exhibit-2B, residential energy intensity (GJ/m2 ) declined at an average annual rate of 1.36% in Canada even when the average household size increased over time**. There is no doubt that bigger and modern washing machines, refrigerators, and sub-zero freezers are making their way into increasingly large houses in Canada, but on net energy efficiency programs and standards have still led to energy savings. A quick calculation demonstrates the result—if residential energy efficiency had remained stagnant at the 1990 level, Canadians would need an additional 400 million GJ or 111 million MWh of energy in 2008. That is equivalent to eliminating four of the largest power plants in the US.

#### 4. Evidence against the rebound effect is seen empirically in the U.S.

Shakeb Afsah 2012 (Shakeb Afsah is the Director of Policy Analysis at the CO2 Scorecard Group and a former environmental economist at the World Bank’s Development Research Group. January 11, 2012. “Energy Efficiency is for Real, Energy Rebound a Distraction,” CO2 Scorecard. <http://co2scorecard.org/Content/uploads/Energy_Efficiency_is_for_Real_CO2_Scorecard_Research_Jan_11_12.pdf> Page: 4 DOA: 11/19/16) CDY

Ironically, the point is reinforced in the United States by similar data used in a Washington Post report to prove the limits of energy efficiency. National data shows that per capita average energy consumption in US homes has barely budged since 1970. But the average American home isn’t representative of energy efficiency measures, as comparative long term per capita residential energy trends of California and Texas show. **California, which has aggressively followed efficiency programs to cut residential energy use, successfully reduced its residential energy use per capita an average of 0.9% per year. In comparison, Texas did not adopt energy efficiency programs and has seen an average increase of 0.4% per year** (Exhibit-3). **That the US per capita average for residential energy has remained stagnant suggests that US as a nation has failed to adopt energy efficiency programs uniformly across all states—a sign of policy weakness not energy Rebound**.

#### 5. Rebound effect exaggerated

Kyle Niemeyer, 2013 [Kyle Niemeyer, He has B.S. and M.S. degrees in Aerospace Engineering from Case Western Reserve University, and is currently a Ph.D. candidate focusing on combustion modeling, “How badly does the rebound effect undercut energy efficiency?,” http://arstechnica.com/science/2013/01/how-badly-does-the-rebound-effect-undercut-energy-efficiency/, accessed 1-30-13, TAP]

Give everyone fuel-efficient cars and we’ll use less fuel, right? According to some economists—and opponents of mandated improvements in energy efficiency—we'll squander some of the savings by driving more. That argument goes for other forms of energy efficiency, suggesting they all can actually lead to greater energy use through a rebound effect. However, **a group of economists and others, led by Kenneth Gillingham of Yale University, argue** in a new Nature commentary **that the rebound effect is exaggerated.** According to their article, **the effect is real but small: 5 to 30 percent of energy savings may be lost due to greater use.** At most, this could reach a little over half of intended savings lost on large scales—but **energy is still saved overall. These numbers are supported by many (“vast” is the word used by the authors) academic studies and simulations.** To be fair, the rebound effect is not simple. It actually comes about via four factors that interact and combine in a complex manner. The first is the “direct” effect, where a drop in the cost of using some energy-consuming device (like a car or washing machine) results in slightly increased use. For cars, various studies show that this reduces savings in energy from the improved efficiency by 5 to 23 percent initially. After everyone becomes accustomed to the lower fuel costs, this could eventually rise to 30 percent.¶ This number is smaller for other devices like home appliances—around 10 percent. How much more often would you use your washing machine if it was more efficient? Would you even notice? The authors argue that these numbers are probably overestimates. People don’t use efficiency directly to gauge how much energy to use, but rather price. That brings the numbers down to somewhere between 5 and 10 percent.

### AT: Political Polarization

#### 1. IoT how??

#### 2. Alt cause

#### 3. Polarization contributes to political involvement

**Alan Abramowitz, 2010** (Alan Abramowitz, professor of political science at Emory, as quoted by Jessica Rettig, contributor to *US News*. May 27th 2010. “Why Political Polarization Might be Good for America,” *US News*, <http://www.usnews.com/opinion/articles/2010/05/27/why-political-polarization-might-be-good-for-america>) ESG

So, are more people more, or less, engaged now than they used to be? **When we look at survey data and voting data, [we see] that people are actually more interested now than they were 10 or 20 years ago. They're getting involved to a greater degree. More people are voting. More people also are talking about politics, and giving money**, and putting out yard signs, and doing things like that. **All the indicators we have show that polarization has actually contributed to increased engagement in politics, because people do perceive important differences and they think that there are big stakes in elections.** So polarization is healthy for our democracy? Well, up to a point. I think that a certain degree of polarization is healthy in a democracy. It clarifies the choices people have in elections, and it helps voters to hold the parties accountable for their performance. **It's healthier to have parties that actually stand for something than to have the situation that we had 50 or 40 years ago, when you really didn't know what the parties stood for because there was so much overlap between them.**

#### 4. Polarization incites more passionate voting

**Gregory Clay 2015** (Gregory Clay, Washington columnist writing for *Inside Sources* and workshop panelist for the National Association of Black Journalists. September 25th 2015. “Counterpoint: The Positive Side of Political Polarization,” *Inside Sources*, <http://www.insidesources.com/counterpoint-the-positive-side-of-political-polarization/>) ESG

**Political polarization also is a surefire way to induce passion among the voting ranks.** Just examine the fan fervor that follows every step taken by Bernie Sanders and Donald Trump and Hillary Clinton and Ben Carson. That fervor likely will translate into huge numbers at the primaries and polls come 2016. We see a clear line of demarcation among our Republican and Democratic and independent presidential candidates, as well as their supporters. No ambiguity. No indifference. No waffling. But **we do see heightened passion and intense debate. Just check the 24 million viewers who watched the Republican debates on Fox News Channel on Aug. 6 and 23 million on CNN on Sept. 16. NFL-type Nielsen numbers for record viewing on cable news outlets. Even 14 months before the presidential election. That’s political polarization at its best. Not its worst.**

#### 5. Polarization can improve the election process

**Diana Epstein and John Graham, 2007** (Diana Epstein, assistant policy analyst at the RAND Corporationand John Graham, dean of the Frederick S. Pardee RAND Graduate School. 2007. “Polarized Politics and Policy Consequences,” *Pardee RAND Graduate School*, <http://www.rand.org/content/dam/rand/pubs/occasional_papers/2007/RAND_OP197.pdf>. Page 17) ESG

**Polarization may also have some advantages for the conduct of political campaigns. When political parties take similar or ambiguous positions on issues, campaigns may focus more on the candidates’ personalities and tactics than on their governing philosophies.** Ambiguous stances may also be advantageous when parties are vulnerable and candidates can concentrate on attracting swing voters, whose concerns may be unpredictable or less extreme. As polarization pulls parties apart, candidates discover that their party affiliation begins to define their ideology and policy positions. **In other words, polarization may help differentiate for voters the substance (not simply the style) of candidates** (Layman et al., 2006). The process of intense, adversarial debate among partisans is distasteful to some people who might prefer a more consensual political culture in which citizens highlight their shared values and downplay deep differences of opinion. But **when politics is used as a vehicle to raise and shed light on authentic issues, it may strengthen the country in the long run.** It may be possible to have a well-functioning representative democracy with strong, polarized parties as long as we have effective procedures that foster public participation and resolve conflict. The framers of the U.S. Constitution devised a set of procedures that have worked fairly well and that may be adaptable enough to endure even the intense period of partisan polarization that we are now experiencing.

#### 6. Doesn’t mean you cannot cooperate – Iran, Israel

### AT: Multilat Solves Climate

#### 1. Trump kills climate policies, like the Paris accord – multilat aint the way

BBC 16(BBC News, May 27th 2016, “Donald Trump would ‘cancel’ Paris climate deal,” <http://www.bbc.com/news/election-us-2016-36401174> DoA:11/20/16) CJV

Republican presidential nominee Donald Trump has said he would "cancel" the Paris climate deal in his first major speech on energy policy. More than 195 countries pledged to reduce carbon emissions in a landmark agreement last year. The billionaire businessman [has said before](http://mediamatters.org/video/2014/01/06/fox-regular-donald-trump-decries-climate-change/197432) there is no evidence that humans are responsible for climate change. He called for more drilling, fewer regulations and the approval of the Keystone XL oil pipeline from Canada. "Any regulation that's outdated, unnecessary, bad for workers or contrary to the national interest will be scrapped and scrapped completely," Mr Trump said. "We're going to do all this while taking proper regard for rational environmental concerns."

#### 2. Multilateralism is dead – besides, it is ineffective

**Global Ethics Corner, 2013** (Global Ethics Corner, part of the Carnegie Council for Ethics in International Affairs. February 25th 2013. “Is Multilateralism Dead?” *Carnegie Council*, [https://www.carnegiecouncil.org/en\_US/studio/multimedia/20130225/index.html/\_view/lang=en\_US](https://www.carnegiecouncil.org/en_US/studio/multimedia/20130225/index.html/_view/lang%3Den_US). Accessed November 20th 2016) ESG

Global problems need global solutions. Just ask members of the G-20 or the United Nations. Both groups were founded on the assumption that multilateral cooperation is key to solving major international challenges. **There's just one problem. Multilateralism isn't working. The last global agreement that included specific commitments and concrete benchmarks was the Millennium Development Goals. That was passed in the year 2000.** Since then, multilateral summits like Doha and Davos have amounted to lots of promises, but little action. Which is why **a growing number of analysts are questioning the merits of multilateralism and advocating something called "mini-lateralism."** Proponents of "mini-laterialism" say **multilateral negotiations have grown too inclusive.** They warn that new actors like the BRICS and NGOs like Oxfam have made the search for common ground on contentious global issues impossible. **More players mean more conflicts and ultimately, less consensus.** So "mini-lateralists" recommend restricting the number of negotiators to those countries actually capable of enacting policy change. In other words, major world powers

#### 3. "Mini-lateralism" is strong and key to solve the warming tipping point- triggers every major impact

**Dellinger '13** ~Myanna Dellinger, Assistant Professor of Law with Western State College of Law and writes on international law with a particular focus on climate change, graduated from the University of Oregon School of Law at the top of her class, Order of the Coif. While in law school, she interned for the United Nations Framework Convention for Climate Change. After law school, she clerked for the late Hon. Francis J. D'Eramo of the Superior Court of the United States Virgin Islands and for the Hon. Procter Hug, Jr., of the United States Court of Appeals for the Ninth Circuit, "Narrowed Constellations in a Supranational Climate Change Regime Complex: The "Magic Number" is Four," [http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=2345938](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2345938" \t "_blank), 10/27/13~

**Just as the world community had almost given up hope for a timely solution to climate change, new events have created reason for cautious optimism that an effective solution may, after all, be found at the supranational scale.** In **2012**, the 195 parties to the United Nations Framework Convention on Climate Change (“**UNFCCC**”) ag**reed that a legal instrument with binding force is to be** adopted by 2015 and **implemented by 2020**.1 In President Barack Obama’s 2013 Climate Action Plan, **the President finally promised that the United States will take international action and lead global climate change efforts**.2 In the spring and summer of 2013, **the United States and China**— arguably the two most important parties to a potential supranational climate change solution—reignited their mutual climate discussions and reached an important **bilateral agreement to jointly phase down hydroflourocarbons** (“HFCs”), one of the most impactful gases in climate change. This and other related rhetoric is indicative of the two nations’ potential willingness to accede to an internationally binding climate change agreement, which in turn may cause a watershed in negotiations and spur further action.∂ **This would be in the nick of time**. Science demonstrating the onset of climate change is increasingly grim: global temperatures reached their highest levels in the history of modern records during the 2001–2010 time period and continue to rise.3 **The decade included a more than 2000% increase in the loss of human life from heat waves,4 not to mention the threatened loss of animal species.** New facts about the diverse problems of climate change continue to surface. In August 2013, for example, the journal Science reported that **shifts in climate are strongly linked to human violence around the world,** such as spikes in domestic violence in India and Australia, increased assaults and murders in the United States**, ethnic violence** in Europe, **land invasions** in Brazil, **police violence** in Holland, and **civil conflicts** throughout the tropics.5 The Fifth Assessment Report by the Intergovernmental Panel on Climate Change (“**IPCC**”) recently **concluded that it is “extremely likely**” (i.e., at 95%–100% certainty) that **human activity is the principal cause of climate change**. Thus, there can no longer be reasonable discussions about whether or not this problem is man-made and, accordingly, about whether or not human action is necessary to solve the problem.6∂ According to the International Energy Agency, carbon dioxide (“CO2”) levels must be **held to 450 parts per million (“ppm”) in this century in order for us to have a chance to keep global warming to the internationally agreed-upon goal of a temperature increase of no more than 2°C.**7 **But in 2013, CO2 levels exceeded 400 ppm for the first time in human history**,8 demonstrating the uphill and urgent battle to be fought on this front**. By putting climate change efforts on hold because of** the **recent global financial crisis and a lack of political will to agree on effective climate change goals**, nations have managed to put the world on track towards a 5.3°C temperature increase with recognized and “potentially disastrous implications in terms of extreme weather events, rising sea levels, and huge [related] economic and social costs.”9 In fact, global temperatures have already risen 0.85°C since 1880.10∂ Because the best predictor of future behavior is often past behavior, **it is doubtful that a large number of nations with** widely **divergent interests i**n the climate context, such as all or∂ most of the 195 members of the UNFCCC, **will be able to reach the required consensus** on a new treaty within the next year, as they have, over the past two decades since the adoption of the UNFCCC, **not been able to agree on significant substantive progress in the area**. The good news is that **they do not all have to**. **Without a doubt, most nations have neither played any significant role in the production of the problem nor do they have much real relevance to its solution.**11 This Article thus argues that **effective climate change action can be instigated by a much lower number of emitters than scholarly and policy-based discussions have promoted thus far, and that** **this is the only realistic solution in the timeframe at hand**. **The “magic number**”12 or “critical mass” **needed to give new impetus to climate action may be as little as just three nations, and is certainly less than “all the major emitters**,” as most legal scholars have so persistently promoted, at least until recently. **Precious time is ticking away. It is now necessary for international lawmakers and scholars to embrace less ideological, but more legally realistic, solutions to this issue, even though such solutions may not represent cosmopolitan ideals of democratic inclusiveness**.13 **The world urgently needs a solution that, in and of itself, can help alleviate at least some of the substantive problem, but that can also secondarily act as a catalyst for further treaty membership or replication**. Some may argue that we do not have time to wait for such a stepped approach. The response to that is that **we have no time to continue promoting and hoping for solutions** that have already proved ineffective. **If we wait for everyone to do something, nothing will happen.**∂ But, which are the most crucial nations to a new climate change leadership constellation? Should a new, narrowed egime complex only include the historical and present major emitters? If so, is it realistic to hope that all of these major emitters will join? Would it be wiser to attempt other compositions such as the inclusion of nations that stand to bear the worst consequences of climate change and nations that seek the most far-reaching solutions, or would this present even worse gridlock? Is it even possible to assess the scientific, political, and symbolic dimensions of the “relevance” of nations in this context?∂ This Article provides answers to the above questions. In doing so, it breaks with scholarly notions that have, by now, proved false. **The Article challenges the viewpoint that all major emitters are needed to form part of a new climate treaty from the beginning. Even just a small handful of nations agreeing on action could cause a shift in the currently stalled talks**. The Article also points out that whereas less-democratic negotiation methods may not be ideal, they serve important pragmatic functions in urgent contexts. In short, the Article promotes and applies a legal realism methodology.∂ The Article first analyz**es factors that have proved crucial to treaty success in recent and more historical contexts**. Much current scholarship examines the same, relatively new, but of course highly relevant, treaties. It provides additional insight from a few of the world’s most successful treaties. **These treaties happen to be of slightly older origins and have thus unfortunately become largely forgotten in today’s apparent rush to reinvent the treaty wheel**. The findings of this Article can **inform today’s treaty decision-making processes, in which parties and scholars often fail to think “outside the box” and learn from what has actually worked** in the past instead of continually promoting solutions that currently do not. Resting on this foundation, the Article proposes a range of narrower constellations for a new regime-complex at the supranational scale that are more likely to be adopted than what has previously been envisioned by scholars and policy-makers. The Article also demonstrates that, in spite of some recent disappointment with the UNFCCC, this is still the most likely and best climate action governance architecture. Finally, the Article identifies nexuses to other international agreements and describes how these may work well as complements to, but not yet substitutes for, a∂ solution under the auspices of the UNFCCC. As the focus of the Article is on treaty development, treaty stipulations, compliance, and review, procedures are not addressed.∂ Much excellent climate change scholarship has been produced in recent years. However, and respectfully, some of it no longer matches reality in international legal proceedings. The Article takes a legal realism approach and posits that **enough theory has been written about who “should” join a new climate change treaty and why; the time has come to look at what can realistically be expected within the near future in this arena**. As has so correctly been said, a **small club of key emitters “could transform the credibility of climate actions and provide an effective alternative to over-ambitious global negotiations prone to [only] yield legal zombies.**”14 The time has come to look at climate treaties in new ways. This Article does so.

### AT: Jacked Energy Prices

#### 1. If energy is not modernized, electric bills would skyrocket by 2050

**Scott DiSavino, 2011** (Scott DiSavino, energy correspondent for *Reuters* covering North American power and natural gas markets. May 24th 2011. “U.S. smart grid to cost billions, save trillions,” *Reuters*,<http://www.reuters.com/article/us-utilities-smartgrid-epri-idUSTRE74N7O420110524>) ESG

\*\*\*Note: EPRI = Electric Power Research Institute

To make the power system of the future a reality, **EPRI, a non-profit electric research and development company**, said power companies need to invest between $17 and $24 billion a year over the next two decades. Much of those costs will be passed onto consumers. "We need to tell power customers there is going to be an improved power system that will result in reduced costs even if they do not see an immediate reduction in their bill," **said Clark Gellings an EPRI Fellow. By the year 2050, EPRI estimated the average electric bill will probably go up by about 50 percent if the smart grid is deployed. If not, Gellings said, the average electric bill could go up by almost 400 percent.** Some of the biggest technology firms in the world are competing to supply the smart grid infrastructure, including International Business Machines, General Electric, ABB, Siemens, Google, Toshiba, Cisco and Microsoft. Last week, Japanese multinational Toshiba agreed to buy Swiss smart grid company Landis+Gyr for $2.3 billion.

#### Hence why remedying infrastructure and prices helps inequality

**David Holt, 2014** (David Holt, reporter for *FuelFix*, news source for analysis on the energy business. January 29th 2014. “Energy is the Key to Solving Income Inequality,” *FuelFix*,<http://fuelfix.com/blog/2014/01/29/energy-is-the-key-to-solving-income-inequality/>) ESG

When exploring solutions to income inequality policy makers pay close attention to the costs. The cost of healthcare. The cost of food. The cost of child care. The cost of housing. What about the cost of energy? According to the Bureau of Labor Statistics, in 2012 the average U.S. family spent over $4,600 or about 9 percent of their budget to heat and power their homes and fuel their vehicles. Families in the bottom fifth of income earners spent nearly 33 percent more of their budget on energy costs than average $2,500 a year or 12% of their annual budget. Reference the chart to the left and you will find that low-income families spend two and half times more on energy than on health services. Unlike food and housing, consumers cannot shop around for the lowest cost energy. Bargains can be found in the supermarket, but, prices at the pump do not vary from one station to the next. Conservation similarly is not an option when it’s a choice between driving to work or saving a gallon of gasoline. **A solution to remedying income inequality is tackling rising energy costs.** The U.S. Energy Information Administration projects the price of electricity will rise 13.6 percent and the price of gasoline by 15.7 percent from now until 2040. Rising global demand**, aging and insufficient energy infrastructure** and restrictive government policies all **play a role in increasing costs.** President Obama has the ability to reverse this trend and lessen the blow to all consumers.

#### 2. Grid modernization could produce $2tril in consumer benefits

**Andrew Kambour, 2014** (Andrew Kambour, senior policy analyst in the Environment, Energy & Transportation Division at the National Governors Association for Best Practices. March 2014. “Governors’ Guide to Modernizing the Electric Power Grid,” *National Governors Association*,<http://www.nga.org/files/live/sites/NGA/files/pdf/2014/1403GovernorsGuideModernizingElectricPowerGrid.pdf>. Page 2) ESG

**Grid modernization** goes beyond current efforts to implement a “smart grid,” in which two-way communications technologies improve the efficiency of grid operations, and **includes the following elements: • Increased communication capabilities and automation on the local distribution grid that can help utilities more quickly respond to outages and redirect power away from affected lines, securely and easily share customer data, ease the transition to greater levels of distributed generation resources, and help utilities prevent and recover from cyber attacks**, (Although, paradoxically, some cyber vulnerabilities stem from an increase in communication and automation devices that connect the grid to the Internet); • **An expanded, technologically advanced, and optimized transmission system that can better integrate utility-scale renewable resources and improve the reliability of the grid; and • Energy storage technologies that can ease the integration of variable renewable resources and provide backup power during outages.** Integrating those technologies and practices into the electric power grid is likely to spur changes in the way electricity is generated, delivered, sold, and consumed. For utilities, states, and consumers, that change represents both opportunities and challenges. **The opportunities—increased reliability and resilience, improved cybersecurity, easier integration of renewable energy resources, and greater use of data— can provide benefits that are estimated at as much as $2 trillion by 2030**, if the interests of consumers, utilities, and state policymakers and regulators are aligned as much as possible. A chief challenge is that fully deploying the technologies associated with a more modern grid calls for a sizable additional investment. Utilities currently spend approximately $34 billion per year on new transmission lines and maintenance on both the transmission and distribution networks. To fully modernize the grid, utilities would need to spend an estimated additional $8 billion to $16 billion per year through 2030. Determining which entities will bear those costs, including how much of the cost utility customers pay, will be a critical factor in how extensively and rapidly the grid is modernized.

#### This is critical because growth alleviates poverty, meaning better access to resources

**Department for International Development 2007** (Department for International Development, a United Kingdom government department responsible for administering overseas aid. 2007. “Growth: Building Jobs and Prosperity in Developing Countries,” *Department for International Development*, <http://www.oecd.org/derec/unitedkingdom/40700982.pdf>. DOA 11/20/16) ESG

Research that compares the experiences of a wide range of developing countries finds consistently strong evidence that rapid and sustained growth is the single most important way to reduce poverty. **A typical estimate from these cross-country studies is that a 10 per cent increase in a country’s average income will reduce the poverty rate by between 20 and 30 per cent.**1 The central role of growth in driving the speed at which poverty declines is confirmed by research on individual countries and groups of countries. **For example, a flagship study of 14 countries in the 1990s found that over the course of the decade, poverty fell in the 11 countries that experienced significant growth and rose in the three countries with low or stagnant growth.** On average, a one per cent increase in per capita income reduced poverty by 1.7 per cent (see Figure 1).2 Among these 14 countries, the reduction in poverty was particularly spectacular in Vietnam, where poverty fell by 7.8 per cent a year between 1993 and 2002, halving the poverty rate from 58 per cent to 29 per cent. Other countries with impressive reductions over this period include El Salvador, Ghana, India, Tunisia and Uganda, each with declines in the poverty rate of between three and six per cent a year.

### AT: PPPs

#### Not that widespread – global number is 3,000

#### World Bank – does not necessarily include privatization

### AT: Corruption

#### 1. Large amount of information are required to combat corruption

**According to Transparency International in 2016,**

**Countries successful at curbing corruption have** a long tradition of government openness, freedom of the press, transparency and **access to information. Access to information increases the responsiveness of government bodies, while simultaneously having a positive effect on the levels of public participation in a country.** Transparency International Maldives successfully advocated for the adoption of one of the world’s strongest rights to information law by putting pressure on local MPs via a campaign of SMS text messages.

#### 2. Technology and data can be used to combat corruption

**Tony Roberts in 2012**,

**All over the world however citizens are fighting back, using new technology to shine a light on fraud and bribery, and to blow the whistle on corrupt practices. In Nigeria the anti-corruption internet database (Acid) has pulled together data and information, tools and resources, and forged a coalition of players to fight the corruption that pervades society.** Their website provides the means to track corruption in public procurement, hosts downloadable training and advocacy materials and interactive tools to enable members of the public to text or tweet reports of corrupt activities live onto Google Maps to raise awareness and to shame perpetrators.

#### 3. The Internet of Things can encourage this – recall the Howard evidence

**Phil Howard et al, 2016** (Phil Howard, professor of technology and international affairs at Oxford University, Christopher Walker, VP of Research and Studies at the National Endowment for Democracy, and Mark Nelson, senior director at the Center for International Media Assistance. January 8th 2016. “Will the internet of things enhance democracy or empower autocrats?” *Democracy Digest*, <http://www.demdigest.org/will-the-internet-of-things-enhance-democracy-or-empower-autocrats>. Accessed Nov 10 2016) ESG

What will this omnipresent connectivity mean for the future of democracy? Soon, we will be fully immersed in a pervasive yet invisible network of everyday objects that communicate with one another. There is evidence that in authoritarian countries, the internet of things will be another tool for social control. Even in democracies, the privacy threats are enormous, as is the potential for political manipulation. **Yet we should also imagine a future of global stability built upon device networks with immense potential for empowering citizens, making government transparent, and broadening information access. If we can actively engage with the governments and businesses building the internet of things, we have a chance to build a new kind of internet—and a more open society.**

#### 4. As an example,

#### Big Data can help make policing more accurate and more transparent

**Cecilia Munoz et al 2016** (Cecilia Munoz, director of the Domestic Policy Council, Megan Smith, US Chief Technology officer at the Office of Science and Technology Policy, and DJ Patil, Deputy Chief Technology Officer for Data Policy and Chief Data Scientist at the Office of Science and Technology Policy. May 2016. “Big Data: A Report of Algorithmic Systems, Opportunity, and Civil Rights,” *Executive Office of the President*, <https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf>. Accessed November 13th 2016. Page 19-20) ESG

The Big Data Opportunity: **Data and algorithms can potentially help law enforcement become more transparent, effective, and efficient.** Law enforcement agencies have long attempted to identify patterns in criminal activity in order to allocate scarce resources more efficiently. New technologies are replacing manual techniques, and many police departments now use sophisticated computer modeling systems to refine their understanding of crime hot spots, linking offense data to patterns in temperature, time of day, proximity to other structures and facilities, and other variables. **The President’s Task Force on 21st Century Policing recommended, among many other steps, that law enforcement agencies adopt model policies and best practices for technology-based engagement that increases community trust and access; work toward national standards on the issue of technology’s impact on privacy concerns; and develop best practices** that can be adopted by state legislative bodies to govern the acquisition, use, retention, and dissemination of auditory, visual, and biometric data by law enforcement.66 Since the Task Force released its recommendations, the White House and the Department of Justice have been engaged in several initiatives to ensure that the report’s recommendations are put into practice across the United States. As part of these efforts, the White House launched the Police Data Initiative to make policing data more transparent and improve community trust.67 More than 50 police departments throughout the nation have joined in this work to realize the benefits of better technology. Commitments from participating jurisdictions include: increased use of open policing data to build community trust and increase departmental transparency, and use of data to more effectively identify policies that could be improved or officers who may contribute to adverse public interactions so they can be linked with effective training and interventions.68 **Consistent with these goals, several police departments in the United States have developed and deployed “early warning systems” to identify officers who may benefit from additional training, resources, or counseling to prevent excessive uses of force, citizen complaints and other problems.** 69 Using de-identified police data, as well as contextual data about local crime and demographics, **these systems are designed to detect the factors most indicative of future problems by attempting to determine behavioral patterns that predict a higher risk of future adverse incidents.** Detecting these patterns opens new opportunities to develop targeted interventions for officers to protect their safety and improve police/community interactions. Separately, some of the newest analytical modeling techniques, often called “predictive policing,” might provide greater precision in predicting locations and times at which criminal activity is likely to occur. Research demonstrates that a neighborhood that has recently been victimized by one or more burglaries is likely to be targeted for additional property crimes in the coming days. An analytical method known as “near-repeat modeling” attempts to predict crimes based on this insight.70 Similarly, a technique known as “risk terrain modeling” can identify specific locations where criminal activity often clusters, such as bars, motels or convenience stores, and can predict the specific social and physical factors that attract would be offenders and create conditions ripe for criminal activity.71 Current Los Angeles Police Department (LAPD) Chief of Police, Charlie Beck, described predictive policing as enabling “directed, information-based patrol; rapid response supported by fact-based prepositioning of assets; and proactive, intelligence-based tactics, strategy, and policy.”72 In some instances these systems have shown significant promise. In experiments conducted by the LAPD’s Foothill Division in which large sets of policing data were analyzed to predict occurrences of crime, the Division experienced a larger reduction in reported crime than any other division in the Department.73

#### 5. Nonunique to the IoT? Like we use this echo chamber trash anyways

#### 6. Nonunique anyways… like Citizens United…

## AFF EXTENSIONS

### EX: Positive Examples

#### Ex. IOT in Rwanda reduced environmental harms and Increased education results

Zhao 2016 (Houlin Zhao, secretary general of the ITU, the U.N. agency for information and communication technologies. November 20 2016. Can investing in connectivity help combat climate change? , *Thomason Reuters Foundation News.* Accessed on November 20, 2016.) DIB

In Kigali, Rwanda, young students had no choice but to stop studying once the sun set because their home had no electricity. In recent years the government and its private sector partners have brought bio gas into homes, a small yet significant part of an overall plan to replace charcoal and firewood with renewables and which now fulfills 85 percent of the Rwanda’s energy needs. Thanks to ICTs monitoring the grid, homes now have more energy for light and school grades have improved.

#### IOT improves the economy in developing countries through entrepreneurs , market connectivity, and Industrial productivity. It also leads to peace

Hartley 2016 (Kris Hartly, professor at Cornell. November 17, 2016. ASEAN’s Broadband Infrastructure Imperative, *The Diplomat.com*, <http://thediplomat.com/2016/11/aseans-broadband-infrastructure-imperative/> . Accessed November 20.) DIB

Information and communications technology (ICT) now appears to be as crucial for economic growth as transportation and energy infrastructure. Footloose entrepreneurs and Internet-savvy consumers are using small-scale mobile applications to create virtual markets and circumvent regulations. At the same time, developing countries are using ICT (Information and Communications Technology) to leap-frog traditional growth stages in boosting market connectivity and industrial productivity. ICT proliferation has even been interpreted as a binding force, with international connections among cities and industrial regions having a pacifying effect on geopolitics. Developing countries in ASEAN have already targeted the productivity boost of urbanization and globalization, and ICT is the next frontier. However, there are significant disparities in broadband reliability and penetration across ASEAN. Efforts to create a structurally cohesive and globally competitive bloc, as embodied by the new ASEAN Economic Community, can be enhanced by regional collaboration in ICT and broadband infrastructure development.