Earth's Electronic Skin

The Internet of Things brings billions of electronic devices into our daily activities, the places we live, and the natural environment. Do we know if we're making the planet smarter—or outsmarting it?

Kasantha Moodley is manager of ELI's Innovation Lab. **Andrew Li** is a baccalaureate student at the University of Virginia taking two degrees, in computer science and economics and public policy.

IN 1989, the president of INTEROP, a networking conference, gave engineer John Romkey a challenge: connect a toaster to the nascent internet, just becoming a part of popular culture. If successful, the engineer would get star billing at the next conference. Romkey and his friend Simon Hackett showed up the following year with a Sunbeam toaster, a simple information database, and a flair for showmanship. They took center stage to grill a slice of bread using a single command. With this innovation, a piece of toast came to represent a slice of our future.

Ten years later, during the dot-com era, sociologist Neil Gross predicted what would come next if we were to connect almost everything to the internet. "In the next century, Planet Earth will don an electronic skin. It will use the internet as a scaffold to support and transmit its sensations. This skin is already being stitched together. It consists of millions of embedded electronic measuring devices: thermostats, pressure gauges, pollution detectors, cameras, microphones, glucose sensors, EKGs, electroencephalographs. These will probe and monitor cities and endangered species, the atmosphere, our ships, highways and fleets of trucks, our conversations, our bodies—even our dreams."

Termed the Internet of Things, or IoT, this technology is now real. It is modernizing our businesses, cities, transportation systems, energy grids, and agriculture. It is also being proposed as the next big thing to confront our most pressing environmental challenges. There are an estimated 25 billion devices connected to the internet. The economic impact of this network, measured as value added, could be anywhere from $3.9 trillion to $11.1 trillion per year in 2025, according to the McKinsey Global Institute.

While all the hype around IoT's economic potential is warranted, we seem to have brushed over the environmental costs—specifically, the unwanted countereffects resulting from increased efficiencies and access to information, or what is now referred to as *digital rebound*. For example, how much energy is consumed by IoT devices, and how does this compare across applications? What is the indirect energy impact of IoT networks at data centers? How is IoT impacting our everyday decisions and long-term behaviors? How can we ensure that this economic boom doesn't inadvertently become an environmental bust, consuming more energy than it saves and creating other pernicious effects? These questions are complex and involve concepts very difficult to measure or predict.

The Network for the Digital Economy and Environment is answering these tough questions. What we call nDEE is an initiative of ELI's Innovation Lab, Yale's School of the Environment, and the Center for Law, Energy, and the Environment at Berkeley law school. With limited empirical research on the environmental costs of IoT, there can be no action taken by businesses, technology developers, or policymakers to ensure the responsible development and deployment of this technology. The nDEE seeks to build a multidisciplinary coalition to produce research that will expand our understanding and encourage actions and policies that harness the benefits of IoT while mitigating its harms.

WHILE IoT devices and their systems are incredibly diverse in their settings and applications, the technological structure is inherently the same, involving layers of perception, networking, and computing. Perception occurs through built-in sensors, networking happens through wireless connections, and computing translates data into specific services required by users. As IoT develops in unexpected ways, this structure will remain largely unchanged. The ubiquity of IoT, combined with its ability to connect with systems and devices anywhere, makes it uniquely powerful.

Smart transportation, for instance, is not only the fastest growing application of IoT, but it will benefit greatly when there is detailed sensory information on every vehicle on the road. The backbone consists of thousands of sensors, cameras, and Radio Frequency Identification (RFID) readers that collect data, which is transmitted through cellular routers. The system then deploys artificial intelligence to use the data to perform an action, such as changing a traffic signal due to an accident. All these components work in perfect harmony and make real-time decisionmaking possible.

The bipartisan infrastructure package could not have been passed at a better time. The act signals a strong push toward digitizing the nation's utilities, transportation, and communications systems

With this data, IoT is already providing a multitude of functions, including real-time analysis of road conditions and congestion, finding parking spaces, and automatically paying tolls. In the future, autonomous vehicles will need to seamlessly integrate this data to plan efficient routes and ensure the safety of passengers by communicating with other IoT-enabled cars. With enough vehicles with IoT capability, some scholars predict, there will be a utopian transportation future. Traffic accidents and congestion will be almost eliminated.

Fully utilizing IoT, transportation's greenhouse gas emissions may decrease anywhere from a low of 5 percent up to perhaps 60 percent, while fuel consumption may decrease anywhere between 30 and 90 percent. The New York City Department of Transportation is testing its Connected Vehicle Pilot Program. The department is procuring hardware and software to implement vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-pedestrian communication. The pilot program will demonstrate how safety-related warnings and other connected-vehicle applications can be deployed in the real world to address safety, mobility, and environmental challenges.

In a similar vein, the ability of electric grids and smart buildings and homes to communicate with each other could illuminate the balance between electricity supply and demand, leading to improved load balancing. Utilities can produce energy based on actual demand, which can refine their strategies on consumer prices and ultimately cut ratepayer costs. Conversely, consumers will be aware of the provider's energy load and can shift use to times when electricity is cheaper. This type of temporal load balancing can reduce stress on grids during peak hours. Another type of load balancing can allow smart grids to schedule power-hungry tasks when solar and wind energy are in high supply.

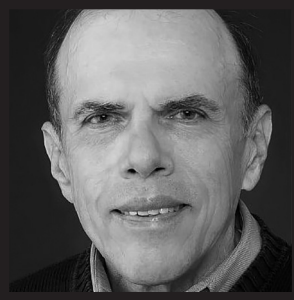
However, automated load balancing at this scale is mostly theoretical. It is not known how responsive people will be to changing their habits. Some studies suggest that consumers' energy consumption behavior is somewhat sticky and may resist rescheduling, even when certain times offer lower prices. But even relatively small cuts can add up. The Department of Energy estimates that if the electric grid were just 5 percent more efficient, the energy savings would equate to permanently eliminating the fuel and greenhouse gas emissions from 53 million cars. To take an example, the energy loss associated with many power plants can be attributed to aging infrastructure, with some assets more than 40 years old. If existing power plants were to be retrofitted with IoT systems, the expected lifetime efficiency savings would total an estimated $50 million per plant. That sounds great, but policymakers will have to consider that new IoT-based power plants of similar capacity would have an expected lifetime efficiency savings almost five times greater. IoT merely confirms the savings of new generation technologies.

With a desperate need for upgrades like this, the bipartisan infrastructure package could not have been passed at a better time. The act signals a strong push toward digitizing the nation's utilities, transportation, and communications infrastructure. With $550 billion allocated for these upgrades, it is a given that IoT will play a key role in many, if not all, of the planned projects. The act even calls for a "Digital Climate Solutions Report" that "assesses using digital tools and platforms as climate solutions, including the Internet of Things." No doubt there will be a plethora of opportunities for IoT. However, any assessment should give due consideration to the system-wide effects and present concerns related to the use of IoT devices. For instance, an analysis of 300 IoT applications by McKinsey found that

Continued on page 30

SIDEBAR

Good Movements Have Downsides Too



Edward Tenner
Distinguished Scholar, Smithsonian Lemelson Center for the Study of Invention and Innovation

"Neither evangelists nor agnostics can always foresee the ultimate, often unintended positive and negative consequences of new systems. Over the decades, good guys and bad guys can be reversed"

The Internet of Things is not a single technology but a movement, an organized campaign for the massive adoption of new standards. Sociologists and anthropologists of information technology have found that movements have a vanguard of enthusiasts and early adopters urging their organizations on the bandwagon—and sometimes confronting a counterforce of skeptics. Careers can depend on which side prevails. But movement thinking is no substitute for imagining all that can go wrong.

Neither evangelists nor agnostics can always foresee the ultimate, often unintended positive and negative consequences of new systems. Over the decades, good guys and bad guys can be reversed. Historians of transportation have reminded us of how utopian the private internal combustion engine once appeared, a solution to the health menace of horse manure and even of dead horses on city streets. In small numbers, automobiles seemed positively benign. Bicyclists had cried out for better roads, helping create cyclist-unfriendly thoroughfares. If the new vehicles began to erode streetcar use, many progressive writers applauded this blow to monopolists. Remember the song for Charles Foster Kane in the film? He "has the traction magnates on the run." Railroads then became environmentally friendly again, until (as the *New Yorker* recently reported) protesters in England have been digging and living in tunnels to prevent damage to a historic forest by a new high-speed line. And vaping, promoted as high-tech harm reduction, has become a new youth addiction.

Sometimes the skeptics turn out to be wrong. The *rebound effect* is a special case of what safety engineers have called risk compensation, the tendency of people living in greater safety to seek out new risks unconsciously. Early in the introduction of mandatory automotive seatbelts some libertarians claimed that a sense of security made buckled-up drivers a greater danger to pedestrians. Later studies showed that seatbelts clearly reduced vehicular deaths. Risk compensation sometimes happens; people in safe financial jobs may seek out "adventure travel." There is a whole book devoted to volcano tourism. But compensation is no iron law.

The real issue for the IoT movement is the unprecedented complexity and fragility of interdependent systems. While many people consider malware the problem, it is not the underlying weakness of the Internet of Things. That instead is a structural problem that first drew attention in the nuclear meltdowns in Three Mile Island and Chernobyl: dangerously fragile links among processes. The Yale sociologist Charles Perrow formulated this analysis in a classic book, *Normal Accidents,* in 1988. Conventional nuclear reactors are a classic example of tight coupling. A failure in one part of the system can create a disastrous cascade of reactions. Supply chain disruptions during the Covid-19 pandemic show what happens when individual nodes of a tightly coupled process are closed down, more than cancelling the intended efficiency of lean global organization. Shipboard safety systems have induced so-called "radar-assisted collisions," like the error that doomed the Italian luxury liner *Andrea Doria* in 1956.

Fortunately the history of technology suggests at least three ways to mitigate the risks of IoT. One is redundancy. Many advanced aircraft are controlled by multiple independently manufactured and programmed computers that compare results. The inevitable glitches in individual systems are outvoted. Another is firebreaks. When Tokyo was the world's largest city in the 18th century it was notoriously fire-prone. The shoguns decreed wide streets and ordered waterways to interrupt the spread of fire. IoT systems should be able to continue functioning if they need to be temporarily disconnected from each other. That points to a third strategy. People must maintain the skills they will need when systems are periodically disrupted. Like commercial airline pilots today, driverless car owners may need to practice on simulators. Even in tomorrow's networked everything, human attention must still be paid.

most data from IoT devices is not used effectively. As an example, only 1 percent of data from an oil rig is regularly examined. The limited data that is actually used is mostly to control anomalies, whereas the real value lies in optimization and prediction, which would allow for significant resource savings.

Agribusinesses are also employing IoT, to reduce water consumption and fertilizer use, cut waste, and improve product quality and yield. By sensing environmental conditions like soil and air temperature, as well as humidity, cost-effective IoT devices can perform analysis such as determining the optimal time to irrigate crops or apply fertilizers or pesticides. This is particularly advantageous in controlled environments. In greenhouses, for instance, IoT devices have access to environment controls like drip irrigation systems, sprinklers to control humidity, or fans and ventilation to control temperature. According to The Nature Conservancy, such precision agriculture can enable farmers to cut water and fertilizer use by up to 40 percent without reducing yields. IoT may also find applications during harvesting, packaging, and distribution to attune farmers to the market, in hopes of reducing food waste. It is estimated that 28 percent of available farmland globally is "reserved" for food waste, as farmers commonly produce more than the market demands to avoid losing profits. Food waste on the farmer's side is a market failure that contributes to hunger, and decomposing food in landfills is a major source of methane emissions. By tracking produce sold using RFID tags, farmers and distributors can model and predict future quantities needed in a given location, leading to an accurate understanding of demand and efficient pricing. This in turn can lead to changes in growing patterns that reduce overproduction and waste at both farms and food retailers.

The direct energy demands will be determined by efficiency innovations, computational improvements, high-speed network technology, and intelligent sleep scheduling of devices

IT WOULD seem that the environmental potential of IoT is unparalleled. However, policymakers need real-world piloting and testing, focused on achieving the energy and environmental resource savings that IoT promises—and avoiding its pitfalls. Even with all these benefits, IoT is not free from environmental costs. Like all electronics, the manufacturing of IoT devices is complex and resource-intensive. In fact, IoT devices are far more problematic than other electronics due to their short lifespan in situ. Battery-powered IoT devices have a limited energy supply, some just lasting a few months. Many devices are designed to fail once the battery dies. Common solutions include low-power networks and smart sleep and wake schedules. Low-power networks, however, severely limit the volume of data transmitted per day to just a few thousand bytes. Increasing the data transfer rate or using a higher-power network like 5G would drastically reduce the lifetime of IoT devices. Added computation complexity, such as security and privacy protections through data encryption, also contributes high energy overhead, resulting in a significant tradeoff between performance of IoT and its environmental impact.

While IoT devices have different uses and thus different energy requirements, there are a few common functions. Powering the microprocessor and sensors and communicating with a wireless network are universal elements, and are also the main consumers of energy. Direct energy usage by IoT devices comes from batteries inside the unit, or more rarely, from the electric grid if the device is plugged in. Extremely low-energy ones may source some of their power from energy harvesters, which provide electricity from ambient sources like solar or thermal energy. Despite the fact that IoT devices generally perform more simple and specialized functions than personal computers and servers—and thus generally require less energy to function—their sheer ubiquity more than makes up for their small size.

While there are no good estimates for the total direct energy use by IoT devices, researchers have observed that while the processing power of electronics has increased steadily, energy efficiency has also doubled roughly every 18 months, a phenomenon known as Koomey's Law. Koomey's Law is a derivative of the more widely known Moore's Law, which states that the transistor count on new processors—and thus, their performance—has doubled roughly every 18 months since the 1970s. Koomey's Law could mean that even as the number of IoT devices and their processing capabilities increase, total energy use by the devices themselves could stay roughly constant for a number of years. With the number of devices expected to grow substantially, we will certainly see how this law plays out for IoT. The direct energy demands of this technology will also be determined by efficiency innovations, computational performance improvements, high-speed network technology, and intelligent sleep scheduling of devices.

Continued on page 32

SIDEBAR

IoT's Environmental Impact Is Up to Us

Stephen Harper
Global Director, Environment and Energy Policy
Intel Corporation

"Society's goal should be to minimize IoT's footprint and maximize its handprint. That comes down to technology design and public policy"

Technologies are tools, and humans determine their net social and environmental impacts by how they are designed and deployed. This is true for the Internet of Things, a poorly understood set of information and communications technology (ICT) solutions that are rapidly proliferating throughout society. Often joined with artificial intelligence, IoT is the enabling technology undergirding everything labeled as "smart"—homes, buildings, transport, cities. Think of a network of sensors, edge computing devices, and data gateways connected via the cloud and data centers. "Digitalization" is a term often applied to this phenomenon.

The environmental and sustainability benefits that IoT delivers have been well publicized, particularly by ICT vendors jockeying for a bigger share of a growing market. Smart homes and buildings, intelligent transportation, precision agriculture, industrial controls, electricity grid resilience, "digital water" . . . the list goes on. A common thread in all these applications is the ability of IoT to turn data into actionable analysis. The International Energy Agency has shown how IoT and other forms of digitalization can be applied to improve the efficiency and lower the climate impact of our energy system.

The potential negative effects of IoT have also received scrutiny, including rising end-of-life e-waste and direct energy consumption. Analysts have also highlighted potential rebound effects, whereby increased energy efficiency and resulting cost savings can lead to increased energy consumption in the long run. Analysis of energy rebounds by the American Council on an Energy Efficient Economy typically minimize the size of such effects, but the potential remains nonetheless.

There is a long history of ICT scary stories, especially concerning predictions of future energy consumption trends. Dating back to the California energy crisis of 2000, which some analysts errantly blamed on the growth of data centers, various "experts" have made claims that ICT devices collectively will consume most or all of the available electricity by some date in the mid-term future. Data centers have garnered the most criticism, although a recent report from Lawrence Berkeley lab shows U.S. data center electricity consumption has leveled off in recent years despite an explosion in the amount of data being processed. More recently, alarms have been raised about the energy threat posed by billions of IoT sensors projected by some date in the future.

A good analytical frame for evaluating the balance of IoT's positives and negatives are the complementary metaphors of *footprint* and *handprint*. The footprint is the direct negative impact (energy, water, climate change) of any person, company, or society. Handprint refers to the enabling impact that technologies can have in helping a person, company, or society to reduce their footprints. ICT technologies, including IoT, definitely have a footprint, but they also present handprint benefits, perhaps more than any other sector of the economy.

Society's goal should be to minimize IoT's footprint and maximize its handprint. That comes down to technology design and public policy. The IEA several years ago convened the Connected Devices Alliance, a consortium of governments and ICT companies, to focus on both. One work product of the CDA is a set of "Design Principles for Energy Efficient Connected Devices" that features 10 recommendations for how IoT and other ICT device makers can minimize the energy footprint of networked devices. In parallel, the CDA issued a set of "Policy Principles for Energy Efficient Connected Devices" that highlight how policymakers can promote handprint innovations and help grow the market for IoT and other network markets.

Several groups are focused on the net benefits of digitalization. ELI itself has convened a conference and series of webinars under their Green Tech banner, with discussions focused on how smart public policies can maximize the net environmental benefits of technology. The Digital Climate Alliance, a coalition of leading ICT companies, has been promoting enabling digitalization policies in legislation on Capitol Hill. By leveraging existing resources, companies and governments alike can push for IoT to be used for good.

The indirect energy use of IoT networks is consumed by routers, switches, and cell towers, as well as end-application devices like cloud servers and data centers. As a whole, networks and data centers consume nearly 400 terawatt-hours per year worldwide, contributing to more than 1 percent of all global electricity use. Some models predict a doubling or tripling of this energy use by the end of the decade, in part due to proliferation of IoT devices. The energy consumption of data centers did, however, plateau between 2010 and 2018, and some researchers attribute this to Koomey's Law. But this may change based on how IoT and its supporting infrastructure develops and influences socioeconomic behaviors in the coming years.

BEHAVIORAL changes resulting from the use of IoT are the most difficult to predict and the most understudied aspect of IoT's impact on the environment. Within the broader scope of environmental policy, scholars have theorized and observed an unexpected behavioral consequence of efficiency gains. Technological changes that increase energy, resource, or time efficiency often have the unwanted side effect of increasing overall consumption levels. This phenomenon has become known as the *digital rebound effect*. There are multiple ways IoT may cause a rebound effect, many of which are rooted in behavioral economics and social factors.

For instance, IoT has shown great potential to cut production costs in industry through increasing efficiency. The result is that industries can produce more goods at a lower cost. Since some of these lower costs are passed on to consumers in the form of lower prices, demand for these goods can rise. This increase is known as the income effect. In manufacturing, this means that while IoT can improve energy efficiency in the production process, these gains may be offset or outweighed by an increase in production overall, creating an energy rebound. Using IoT to improve energy efficiency can actually have an undesired impact on total energy use, or at least a smaller positive impact than expected.

Many researchers have advocated for a distributed model of governance. International organizations, national governments, and individual corporations may all have a hand in managing IoT systems

Additionally, there are other environmental concerns the manufacturing process may create that aren't balanced by efficiency improvements. For example, an IoT system in a factory may significantly reduce electricity use from machines on standby mode, decreasing the factory's costs and resulting in increased production levels. However, the IoT system may not decrease the amount of non-energy-related pollution generated or the volume of raw materials consumed per unit. Thus, while increased electricity use from increasing production may be countered by better energy efficiency, other environmental costs may not be.

The rebound effect is also created through substitute and complement services. A good is a complement of another if the demand for one good increases when the demand for the other increases. For example, peanut butter and jelly may be complements of each other since they are often consumed together. This theory can be applied to IoT applications as well. If an IoT system supplements rather than replaces existing behavior, and thus acts as a complement rather than a substitute, then consumption may be drastically increased through both traditional activity and novel IoT activity. For instance, online shopping could be a complement to in-store shopping, and IoT may boost both types of purchases. Or, more likely, it may be found that AI models and IoT systems complement each other. As IoT systems proliferate, more AI models are trained to capitalize on the data generated from them. Training some AI models can emit as much carbon as five cars in their lifetimes. Thus, the rebound effect for complements is much greater and more likely to result in environmental backfire than substitutes. Unfortunately, the study of complements in the context of the digital rebound effect is nearly nonexistent despite its likely implications.

Another lesser-known rebound effect is the skill rebound, which in effect reduces the need for qualifications or skills to perform certain activities, thanks to digitization. With the autonomous vehicle example, driverless cars could mean anyone, regardless of age or driving ability, could get in a car and "drive," resulting in more cars on the road.

Rebound effects seem to be the rule rather than an exception and cannot be ignored when assessing the total environmental impact of IoT or any other technological innovation. There have been early attempts at estimating the direct rebound effects of specific programs and policies, which have been found to be 10 percent or less. However, it should be recognized

that these estimates are based on varied assumptions and methods, resulting in some uncertainty. More recent research is focused on assessing the accuracy of existing methodologies and proposing solutions that would ensure scientifically robust assessments. As IoT faces a constant push and pull between its positive and negative effects, sound research will be critical to our understanding of IoT's rebound effects. These effects should be considered an open question, one that should be continually asked, especially given the rapid pace of digitalization, which has been further accelerated by the Covid-19 pandemic.

WILL IoT become yet another burden on our planet, or will it be its long-awaited savior? Tipping the scales on this duality will be the policies and standards that frame the IoT ecosystem as a whole, or IoT governance. Due to the distributed, decentralized, and global nature of IoT, there are no clear governance organizations or definitive goals or guidelines. Many researchers have advocated for a distributed model of governance, where responsibility is spread both vertically by hierarchy and horizontally by geography or sector. International organizations, national governments, and individual corporations may all have a hand in managing IoT systems.

The study of IoT today is critical in developing the capabilities of IoT tomorrow. We still have time to ensure that the environmental impact is not a side effect, but a primary feature of the data revolution

While such a complex, global, and hierarchical IoT governance system is still in the initial stages of framing, existing governance systems and institutions may help guide its development. IoT governance can rely at least partially on established entities like international standards-setting organizations, or SSOs. The International Organization for Standardization, International Electrotechnical Commission, and International Telecommunication Union play a large role in the governance of information and communications technology by setting global, generally voluntary technical standards.

The work of these organizations and others like them has led to extremely effective governance of the internet, a sector closely related in scope and nature to IoT. Thus, internet governance can be instructive for IoT governance. Governance of the internet is multilayered and hierarchal, with international standards and protocols established by SSOs (i.e., Wi-Fi, HTTP), regulations and laws enacted by governments (i.e., General Data Protection Regulation), privacy policies and technical limits set by companies, and even individual restrictions like parental controls. The same governance structure will likely be applied to IoT.

The environmental benefits and harms of IoT are often seen as just a technological issue, rather than a governance issue. Optimists believe that IoT has the potential to be a boon for the environment, so much so that they think technological improvements will eventually arc toward sustainability without the need for regulation.

The other issue is that there can be no governance without facts. Simply put, the problem is not well defined, and current research of IoT and the environment is lackluster. Many academic papers frame IoT as an economic boon, while overlooking its environmental costs. Robust research at this intersection is crucial for technological improvements. Good governance will thus catalyze research that provides powerful empirical data on IoT's second-order and third-order impacts; promote the exploration of methodologies to better understand and estimate the system-wide impacts; and facilitate an inclusive and interdisciplinary community of practice.

Despite the proliferation of billions of IoT devices since the 1990s, researchers and industries have only recently begun to pay attention to their large-scale benefits and harms. Predictions that IoT can single-handedly save or destroy the environment are at the very least premature. Some IoT applications will persist and propagate, while others will enjoy only momentary hype. The ones that prove durable will have effects beyond those that were intended and be subject to diverse and global economic, behavioral, and cultural influences.

The current research gap, particularly in the quantifiable environmental effects and long-term direction of IoT, leaves much of the future of IoT and the environment up to fate. But because we have yet to define its future, this destiny is malleable. The study and discussion of IoT today will be critical in developing the fundamental capabilities and priorities of IoT tomorrow. We still have time to ensure that the environmental impact is not a side effect, but a primary feature of the IoT revolution. **TEF**