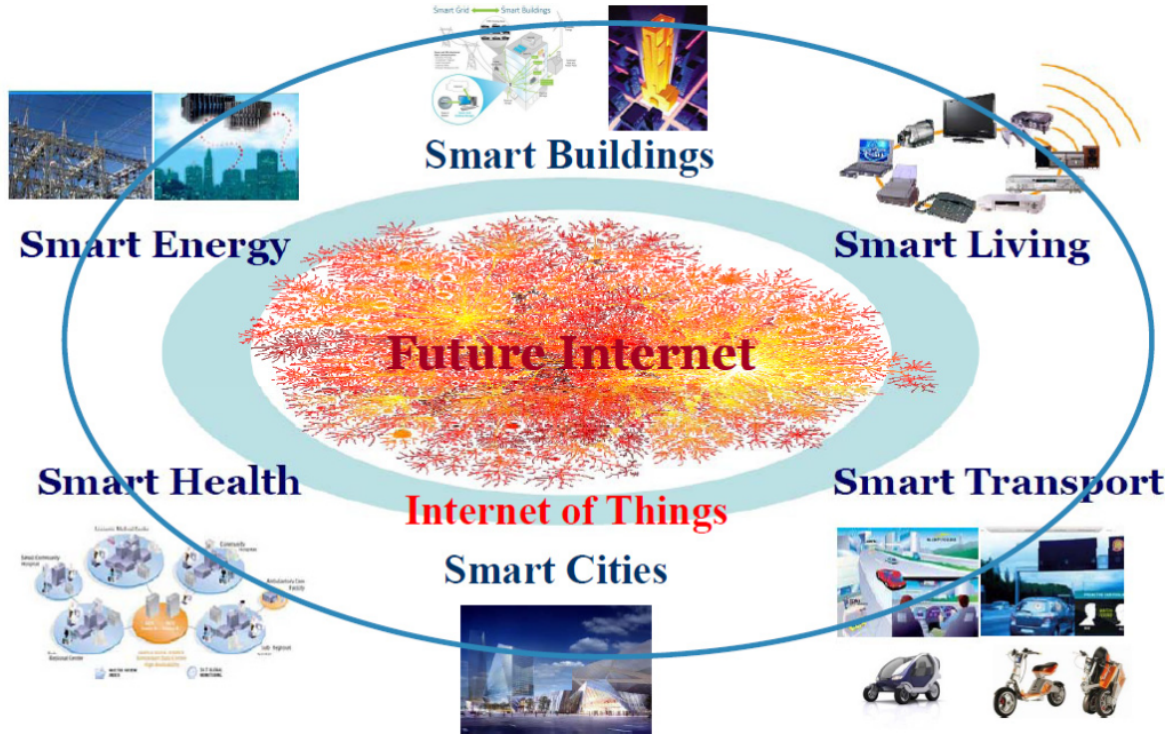

Forbes: How The IoT Enables Pushbutton Regulation From A Distance

The Internet of Things (IoT) is designed as a command-and-control system to regulate the entire system in which they operate. This includes humans contained therein as well.

This article's author rightly concludes,

> *The "Smart Cities" movement potentially may present the most significant incarnation of Regulation from A Distance, though. Versions I've noticed seem to involve heavy governmental control, "partnered" with large corporations or government-preferred players.*

 TN Editor

Artificial intelligence can be curiously stupid. My Android phone still thinks I'm "wing Cruz" and doesn't know my kids. Pandora overplays

The Church and Deadmau5 (no offense).

As hackable as Alexa, Jeep Cherokees and credit card services are over a public Internet not designed for security, the networked gadgetries enabled by the Internet of Things (IoT) continue to dazzle. An overwhelming number of them will be on display again in January at the 2020 Consumer Electronics Show (#CES2020).

The primary vulnerability of the IoT is not hackers, though, but IoT policy.

Technology that overcomes "market failure" in the provision of goods and services should enable the reduction and streamlining of regulatory burdens. Instead it sometimes threatens to foster the expansion of government power.

That is, the same IoT that animates objects can also mean instantaneous nanny-state regulation from a distance—of drones, vehicles, buildings, social media use, schooling and more.

You've heard of free-range kids vs. helicopter parenting?

Well, the society fancying itself on the verge of flying cars may face helicopter government instead; assorted bureaucrats clicking and swiping from afar, using the IoT to control the IoT.

It's one thing for Tesla to send its own software updates to its customers' cars. We definitely want such things to happen—a lot.

But as Jason Dorrier noted in Singularity Hub, "regulations … written into software" could be highly appealing to regulators. A "No drones within 100 feet of federal buildings," rule, for example, could be enforced by requiring the uploading to networked objects of software patches altering GPS coordinates, and disabling them in event of non-compliance.

Dorrier named other examples: software patches imposing speed restrictions and no-drive zones on vehicles, preventing cars from starting without seatbelt attachment, and mandating thermostat settings and water use restrictions in buildings.

Entrepreneur Marc Andreessen long ago described software eating the world. Titans in sectors from “movies to agriculture to national defense” are now software companies, run on software and delivered as online services.

Unfortunately, while software has eaten business models, it is not eating traditional top-down central regulatory regimes in the sense of displacing them.

Those systems are preparing to eat the IoT instead.

The next step in this “evolution” could go beyond rules mandating the updating or patching of software, to unelected bureaucrats simply doing it themselves remotely by clicking and swiping rather than enacting a law or rule, Constitution notwithstanding. The use of guidance documents, informal directives and other “offers you can’t refuse” are already a prominent regulatory concern highlighted by the Administrative Conference of the United States. The IoT could magnify such abuse.

Read full story here…