GlobalResearch
Center for Research on Globalization

Digital Electronic "Internet of Things"(IoT) and "Smart Grid Technologies" to Fully Eviscerate Privacy

By James F. Tracy
Global Research, February 02, 2015

Region: USA
Theme: Intelligence, Police State & Civil Rights, Science and Medicine

The "Internet of Things" (IoT) and Smart Grid technologies will together be aggressively integrated into the developed world's socioeconomic fabric with little-if-any public or governmental oversight. This is the overall opinion of a new report by the Federal Trade Commission, which has announced a series of "recommendations" to major utility companies and transnational corporations heavily invested in the IoT and Smart Grid, suggesting that such technologies should be rolled out almost entirely on the basis of "free market" principles so as not to stifle "innovation."[1]

As with the Food and Drug Administration and the Environmental Protection Agency, the FTC functions to provide the semblance of democratic governance and studied concern as it allows corporate monied interests and prerogatives to run roughshod over the body politic.

The IoT refers to all digital electronic and RFID-chipped devices wirelessly connected to the internet. The number of such items has increased dramatically since the early 2000s. In 2003 an estimated 500 million gadgets were connected, or about one for every twelve people on earth. By 2015 the number has grown 50 fold to an estimated 25 billion, or 3.5 units per person. By 2020 the IoT is expected to double the number of physical items it encompasses to 50 billion, or roughly 7 per individual.[2]

The IoT is developing in tandem with the "Smart Grid," comprised of tens of millions of wireless transceivers (a combination cellular transmitter and receiver) more commonly known as "smart meters." Unlike conventional wireless routers, smart meters are regarded as such because they are equipped to capture, store, and transmit an abundance of data on home energy usage with a degree of precision scarcely imagined by utility customers. On the contrary, energy consumers are typically appeased with persuasive promotional materials from their power company explaining how smart meter technology allows patrons to better monitor and control their energy usage.

Almost two decades ago media sociologist Rick Crawford defined Smart Grid technology as "real time residential power line surveillance" (RRPLS). These practices exhibited all the characteristics of eavesdropping and more. "Whereas primitive forms of power monitoring merely sampled one data point per month by checking the cumulative reading on the residential power meter," Crawford explains,

> modern forms of RRPLS permit nearly continued digital sampling. This allows watchers to develop a fine-grained profile of the occupants' electrical

> appliance usage. The computerized RRPLS device may be placed on-site with the occupants' knowledge and assent, or it may be hidden outside and surreptitiously attached to the power line feeding into the residence.
>
> This device records a log of both resistive power levels and reactive loads as a function of time. The RRPLS device can extract characteristic appliance "signatures" from the raw data. For example, existing [1990s] RRPLS devices can identify whenever the sheets are thrown back from a water bed by detecting the duty cycles of the water bed heater. RRPLS can infer that two people shared a shower by noting an unusually heavy load on the electric water heater and that two uses of the hair dryer followed.[3]

A majority of utility companies are reluctant to acknowledge the profoundly advanced capabilities of these mechanisms that have now been effectively mandated for residential and business clients. Along these lines, when confronted with questions on whether the devices are able to gather usage data with such exactitude, company representatives are apparently compelled to feign ignorance or demur.

Yet the features Crawford describes and their assimilation with the IoT are indeed a part of General Electric's I-210+C smart meter, among the most widely-deployed models in the US. This meter is equipped with not one, not two, but three transceivers, the I-210+C's promotional brochure explains.[4]

One of the set's transceivers uses ZigBee Pro protocols, "one of several wireless communication standards in the works to link up appliances, light bulbs, security systems, thermostats and other equipment in home and enterprises."[5] With most every new appliance now required to be IoT-equipped, not only will consumer habits be increasingly monitored through energy usage, but over the longer term lifestyle and thus behavior will be transformed through power rationing, first in the form of "tiered usage," and eventually in a less accommodating way through the remote control of "smart" appliances during peak hours.[6]

Information gathered from the combined IoT and Smart Grid will also be of immense value to marketers that up to now have basically been excluded from the domestic sphere. As an affiliate of WPP Pic., the world's biggest ad agency put it, the data harvested by smart meters "opens the door to the home. Consumers are leaving a digital footprint that opens the door to their online habits and to their shopping habits and their location, and the last thing that is understood is the home, because at the moment when you shut the door, that's it."[7]

As the FTC's 2015 report makes clear, this is the sort of retail (permissible) criminality hastened by the merging of Smart Grid and IoT technologies also provides an immense facility for wholesale criminals to scan and monitor various households' activities as potential targets for robbery, or worse.

The FTC, utility companies and smart meter manufacturers alike still defer to the Federal Communications Commission as confirmation of the alleged safety of Smart Grid and smart meter deployment. This is the case even though the FCC is not chartered to oversee public health and, basing its regulatory procedure on severely outdated science, maintains that microwave radiation is not a threat to public health so long as no individual's skin or flesh have risen in temperature.

Yet in the home and workplace the profusion of wireless technologies such as ZigBee will compound the already significant collective radiation load of WiFi, cellular telephony, and the smart meter's routine transmissions. The short term physiological impact will likely include weakened immunity, fatigue, and insomnia that can hasten terminal illnesses.[8]

Perhaps the greatest irony is how the Internet of Things, the Smart Grid and their attendant "Smart Home" are sold under the guise of convenience, personal autonomy, even knowledge production and wisdom. "The more data that is created," Cisco gushes, "the more knowledge and wisdom people can obtain. IoT dramatically increases the amount of data available for us to process. This, coupled with the Internet's ability to communicate this data, will enable people to advance even further."[9]

In light of the grave privacy and health-related concerns posed by this techno tsunami, the members of a sane society might seriously ask themselves exactly where they are advancing, or being compelled to advance to.

Notes

[1] Federal Trade Commission, Internet of Things: Privacy and Security in a Connected World, Washington DC, January 2015. Accessible at http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[2] Dave Evans, "The Internet of Things: How the Next Evolution of the Internet is Changing Everything, Cisco Internet Business Solutions Group, April 2011, 3. Accessible at http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[3] Rick Crawford, "Computer Assisted Crises," in George Gerbner, Hamid Mowlana and Herbert I. Schiller (eds.) *Invisible Crises: What Conglomerate Control of Media Means for American and the World*, Boulder CO: Westview Press, 1996, 47-81.

[4] "I-210+C with Silver Spring Networks Micro-AP" [Brochure], General Electric, Atlanta Georgia. Accessible at http://www.gedigitalenergy.com/app/Resources.aspx?prod=i210_family&type=1

[5] Stephen Lawson, "ZigBee 3.0 Promises One Smart Home Standard for Many Uses," *pcworld.com*, November 16, 2014.

[6] One of the United States' largest utilities, Pacific Gas & Electric, has already introduced tiered pricing to curb energy usage in summer months during "high demand" times of the day. http://www.pge.com/en/myhome/saveenergymoney/plans/smartrate/index.page

[7] Louise Downing, "WPP Unit, Onzo Study Harvesting Smart-Meter Data," *Bloomberg.com*, May 11, 2014.

[8] Sue Kovach, "The Hidden Dangers of Cellphone Radiation," *Life Extension Magazine*, August 2007; James F. Tracy, "Looming Health Crisis: Wireless Technology and the Toxification of America," *GlobalResearch.ca*, July 8, 2012.

[9] Evans, 6.

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: **James F. Tracy**
https://jamesftracy.wordpress.com/

About the author:

James F. Tracy was a tenured Associate Professor of Journalism and Media Studies at Florida Atlantic University from 2002 to 2016. He was fired by FAU ostensibly for violating the university's policies imposed on the free speech rights of faculty. Tracy has filed a federal civil rights lawsuit against the university, with trial set to begin November 27, 2017. Tracy received his PhD from University of Iowa. His work on media history, politics and culture has appeared in a wide variety of academic journals, edited volumes, and alternative news and opinion outlets. Additional information is available at MemoryHoleBlog.com, TracyLegalDefense.org, and jamesftracy.wordpress.com.