The phrase *internet of things* (IoT) identifies any physical devices' existing & inherent potential to obtain an IP address fit for remote, internet-based control. Definitions aside, IoT represents the new era of wi-fi-enabled manufacturing, commercial, residential, and personal hardware. The IoT connection to a common network of communication in the web enables the automation of many human tasks. For example, the nightly task of turning on the lights may now be replaced by a program to illuminate household lights, based on proximity to a wearable device like a Fitbit. Likewise, industrial, commercial, and other sectors of the economy may now implement such automation, much to the chagrin of the employees currently fulfilling those tasks.

The great consequence of IoT is the risk of unauthorized control of security, data-sharing, privacy control[1], and general exposure to the world wide web. The most illustrious example is that of the Stuxnet virus that was developed to infect the network system running the Iranian nuclear centrifuges—the which were remotely controlled to incorrectly spin causing massive physical destruction and slightly slowing the Iranian nuclear program. Data-sharing perils generated by IP-accessible products include medical data, HIPAA-protected data, identity and financial data are increasingly exposed to the web, starting with the electromagnetic credit card features to smart-pay and ending with biologically-integrated chips—in which case our own bodies become an IoT product. There are an estimated 7.3 billion devices needing security updates in the next three years[2]. Lastly, privacy control remains a ubiquitous feature of the internet, and therefore IoT merely exaggerates an existing problem. For example, home IoT-enabled cameras may be hacked just as a cell-phone camera, and private conversations may be hacked from listening devices like Google Home. Implicit within these perils is the potential for ransom and extortion, case in point recent, global-wide ransom attacks.

The great potential of IoT remains the various attempts to harness this massive influx of new data. Artificial Intelligence may be called upon for such a task. Currently, the gargantuan task likes in the collection, cleaning and manipulation of structured and unstructured, private and public data. IoT exponentially increases the data *per unit sensors* connected by IP address. They say data science is the number one job, and now I better understand why.

---

[1] https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#73ce4cf41d09

[2] http://www.wired.co.uk/article/internet-of-things-what-is-explained-iot