The Internet of Things & Applications

If objects have a life that is innate, what would happen if these objects go further and were capable of storing data, sensing the environment and communicating with each other? That is the kind of life that the Internet of Thing offers to new electronic devices.

The Internet of Things (IoT) is the “network of interconnected sensor-equipped electronic devices that collect data, communicate with each other, and can be monitored or controlled remotely over the Internet” (Ahrens, “Making Sense of the Internet of Things”). The main goal of the IoT’s development is to connect the physical world and the environment to the Internet or to wireless networks, this would allow making objects, machines and work environments interactive. By using sensors, objects will be capable of exchanging data with other machines without the need of human intervention (Heires, “Preparing for the Internet of Things”). The IoT includes different technology infrastructure, devices and services such as the cloud, computing, data analytics and mobile communications. The IoT is not a prediction; it is a plausible trend that is moving forward, rapidly. It is estimated that by 2020, 50 billion devices around the world will be connected to the Internet. “A third of them will be computers, smartphones, tablets and TVs… The remaining two-thirds will be other kinds of things: sensors, actuators, and newly invented intelligent devices that monitor, control, analyze, and optimize our world (Burkitt, “A Strategist’s Guide to the Internet of Things”). There are major platforms and discoveries that have had a rich wage of complexity, global reach and novelty. But the IoT is for sure a trend that takes the development of interconnectivity to another level, one that once was only imaginable.

There will be a gigantic range of interconnected systems and products that the IoT will enable, from simple monitoring of home temperature and security to the quantified self … to fully networked factories and hospitals, to automated cities”. (Burkitt, “A Strategist’s Guide to the Internet of Things”). While it is true that the IoT will signify a major shift in the economy, politics and regulations from all government agencies, companies, and non-profit organizations, this paper will only focus on the effects that it will have on citizens by arguing that, although the development of the IoT is still on early phases regarding its development and spread, it is potentially a threat to both security and privacy.

Since the IoT is a rapidly growing trend, most major companies are seeking to get involved, there are enormous efforts to trigger this trend as something positive in the forthcoming future. A frequent discourse that is present in the media mentions the major positive technological improvement that the IoT represents. “Capitalist societies generally educate people to appreciate the conveniences and choices of modern consumer technologies” (Parks and Starosielski, 6). Who wouldn’t want a refrigerator that could tell you when you are running out of milk or that you need to replace one of its pieces? How fantastic it would be that your car could save information about what routes you take every day? Who would not want a house that can monitor and regulate the temperature to save energy? Or a watch that can save your sleep pattern information? These are all conveniences that are presented to potential consumers about the IoT, however little is said about what happens to all this information that is saved by the devices and whether this is safe or could be a treat for the consumers´ privacy.

If all devices are connected to the Internet, this means that they are vulnerable to be hacked. A recent study from HP titled “Internet of Things State of the Union” exposed relevant information that makes us more sceptical about relying on IoT as a safe technology. Some of the facts that the study revealed are that 70% of IoT devices were vulnerable to attack, 90% of the devices that were used for the study collect at least one piece of personal information via the device, the cloud, or its mobile application, 6 out of 10 devices that provide user interfaces were vulnerable to a range of issues and had weak credentials, 80% of devices along with their cloud and mobile application components failed to require passwords or a sufficient complexity and length and 70% of the devices along with their cloud and mobile application enable an attacker to identify valid user accounts through account enumeration (“Internet of Things Research Study Report”). Many devices connected to the Internet collect valuable personal information from users, such as name, address, date of birth, health information and credit cards numbers. What the HP study reveals is that all this information is vulnerable to potential hacker attacks.

The fact that the infrastructure that supports the Internet-connected devices is unreliable and can fail represents a disadvantage to the IoT as well. The infrastructure that supports the Internet works differently across diverse geographical areas. For example, in Mexico Telmex has the monopoly as the company that provides Internet to users and companies. It is expensive, unreliable and it fails frequently. Users can spend hours or days without Internet, and Telmex’s support team is inefficient and fickle. Furthermore, since the Internet service is expensive, many individuals do not have this service, therefore the IoT could increase the damage caused by the digital divide.

## CONCLUSION

Finally, there is the environmental impact that the development and spread of the global IoT will bring. “In 2007 media technologies were responsible for between 2.5% and 3% of the world’s greenhouse gas emissions, a figure that has only increased with the expansion of Internet infrastructure, emergence of new data centres, and intensified production and use of consumer electronics” (Parks and Starosielski, 14). If we take into consideration this information and the fact that by 2020, 50 billion devices around the world will be connected to the Internet, it is crucial that we think about the environmental impact that the IoT will cause and question what can be done to prevent it.

The IoT will be here sooner rather than later, for now it is a trend that is running fast to become a reality. Under this fact it is essential that we demand public access to technological knowledge about the IoT. Technology moves faster than the development of proper legal measures and action to regulate it. We need to ask how can we be certain that the IoT is something that will not harm our privacy and safety. Who is building this technology and who owns it? What institutions could we approach in case of concern or discomfort? Where is the line between what is legal and what is illegal? How much information are we willing to provide/compromise to these interconnected devices? What happens if we choose not to participate in this technology? What is it necessary to arise greater public interest in what are the implications of the interconnectivity of all the devices that rule our environmental daily life and habitus? All these questions are genuine and each one of them deserves an answer.