IOT
chapter -11
ETHICS

Q1) summarize what the Internet of Things is?

According to technologist and policymaker Vannevar Bush:

- *[Machines with interchangeable parts can now be constructed with great economy of effort.*
- *In spite of much complexity, they perform reliably.*
- *Such as typewriter, or the movie camera, or the automobile.*
- *Electrical contacts have ceased to stick when thoroughly understood.*
- *Note the automatic telephone exchange, which has hundreds of thousands of such contacts, and yet is reliable.*
- *The world has arrived at an age of cheap complex devices of great reliability; and something is bound to come of it.]*

- The availabilities of technology brings certain abilities within the reach of not just the powerful but the ordinary citizen.
- Earlier examples were concerned with publication, transport, and communication.
- The advances in the Internet of Things are also primarily related to communication, but now allow the publication and transmission of vast streams of data, from the social to the environmental without needing the permission or expertise of a technological or political elite.
- The "form follows function" applies primarily to the physical usage of the "Thing", its affordances, sensors, and actuators, and only minimally to its digital communications.
- This leads to objects that can look innocuous (harmless) but have arbitrary and potentially unexpected capabilities.
- Connecting the Internet to the real world allows both your physical actions to be made public and, in the opposite direction, for events on the Internet to affect your environment.
- Applying this bidirectional communication to Things can lead to features that interact with the concept of privacy. When you switch on your Good Night Lamp, the "little lamp" at your mother's bedside will also turn on, letting her know you are home.
- When you leave the office, the WhereDial at home turns to let your partner know you're travelling.
- We have repeatedly noted that the Internet of Things is made up of
- Physical object + controllers, sensors, and actuators + Internet service
- Each of these aspects has a part to play in the ethical issues specific to the Internet of Things.

Q2) Explain the issues on PRIVACY. Also explain how internet affects PRIVACY.

- The Internet, as a massive open publishing platform, has been a disruptive force as regards the concept of privacy.
- Everything you write might be visible to anyone online.
- There is a *value* in making such data public: the story told on the Internet becomes your persona and defines you in respect of your friends, family, peers, and potential employers.
- A common argument is "if you've got nothing to hide, then you've got nothing to fear."

- You *change* and your persona changes.
- Yet your past mistakes (drunken photos, political statements) may be used against you in the future.
- As the Internet of Things is about *Things*, which are rooted in different contexts than computers, it makes uploading data more ubiquitous.
- Even innocuous photos can leak data. With GPS coordinates (produced by many cameras and most smartphones) embedded into the picture's EXIF metadata, an analysis of your Flickr/Twitpic/Instagram feed can easily let an attacker infer where your house, your work, or even your children's school is.
- Similar issues exist with sports-tracking data, whether produced by an actual Thing, such as Nike+ or a GPS watch.
- This data is incredibly useful to keep track of your progress, and sharing your running maps, speed and heartbeat.
- It may be trivial for an attacker to infer where your house is (probably near where you start and finish your run) and get information about the times of day that you are likely to be out of the house.
- To the extent that you allow your location to be shared with people you've *chosen* to share it with, there is no infringement of privacy.
- We saw previously that many "things" have little in their external form that suggests they are connected to the Internet.
- It is very important to note that even aggregate data can "leak" information.
- If you can see data collected for a street, for example, then comparing a week when a household is away on holiday with a normal week when they are at home might tell you about their usage.
- Some very interesting questions can be raised about this: should companies be prevented from trading data with each other?
- Should there be legal limits to what data can be kept or what analyses performed on it?
- Or do we have to think the unthinkable and admit that privacy is no longer possible in the face of massive data combined with data mining?
- As sensors such as CCTV cameras, temperature meters and Bluetooth trackers are installed in public and private spaces, from parks to shops, data about you is collected all the time.
- The term "data subject" has been coined for this purpose. Although you may not own the data collected, you are the subject of it and should have some kind of rights regarding it: transparency over what is collected and what will be done with it, the access to retrieve the data at the same granularity that it was stored, and so on.

Q3)Who CONTROLs data collected by devices (sensors)?

- Some of the privacy concerns manifest only if the "data subject" is not the one in control of the data.
- For example if the drunken photo was posted by *someone else*, without your permission.
- This is a form of cyberbullying, which is increasingly prevalent in schools and elsewhere.
- If you are gifted a WhereDial or a Good Night Lamp, is there an *expectation* that you use it, even if you don't really want to?
- While the technology itself doesn't cause any controlling behaviour, it could easily be applied by a spouse/parent/employer in ways that manifest themselves as abusive, interfering, or restrictive.

- Already, companies and organisations are looking at mashing up data sources and apps and may start to offer financial incentives to use Internet of Things devices: for example, reductions in health insurance if you use an Internet-connected heart monitor, have regular GPS traces on a run-tracking service, or regularly check in to a gym.
- As with questions about privacy, there are almost always good reasons for giving up some control.
- From a state perspective, there may be reasons for collective action, and information required to defend against threats, such as that of terrorism.
- The threat of one's country becoming a police state is not merely a technological matter: institutions such as democracy, the right to protest, free press, and international reputation should balance this.
- Now that surveillance equipment is cheap, and the processing power required to *analyse* the mountain of data produced by this equipment gets ever more accessible.
- As the Canadian open government activist David Eaves has eloquently discussed, it is not only authoritarian states such as Iran and China which are intent on controlling their Internet but also democratic ones.
- The US, UK, Canada, France, and others have already enacted various laws to give the state and its favoured corporations greater control over its citizens' use of the Internet.
- Of course, it may not be "the State" that profits from the control but corporations.
- Companies have the expertise and the technology to interact with the Internet. This is particularly true of the Internet of Things, which has largely been driven by monitoring and logistics concerns within large businesses.

Q4)Explain the terms "DISRUPTING CONTROL" and "CROWDSOURCING".

- **DISRUPTING CONTROL**
- The other major possibility that Eaves suggests is that "The Internet Destroys the State".
- When we refer to a technology as "disruptive", we mean that it affects the balance of power.
- If one of the fears about the Internet of Things is that it will transfer power away from the citizens, the subjects of technology, to the elite, then perhaps it can also be used to redress that balance.
- One extreme example of this would be how surveillance and fears of the Big Brother state (CCTV cameras, remote-controlled helicopter-drones) might be mitigated by "sousveillance".
- Here, activists might have compromised public cameras, or perhaps installed additional spy cameras, routed through self-healing networks in people's homes, hidden in public spaces, flying in the airspace, or even crawling the sewers.

- **CROWDSOURCING**
- One fascinating feature of modern Internet life is "crowdsourcing", from knowledge to funding projects to work.
- In the Internet of Things world, this concept has manifested itself in sensor networks such as Xively.
- Founder Usman Haque has said that their original intent wasn't simply "making data public" but also letting "the public making data".
- Governments and companies simply do not and cannot have a monopoly on all recording of data: there are infinite combinations of data sources.

- Choosing which data to record is a creative and engaged act, as well as, perhaps, a political one.
- Former Xively evangelist Ed Borden has led a "call to arms" for a citizen-led air-quality sensor network.
- As he points out, "The air quality data collected by the government is likely sampled from far, far away and then applied to you on a regional level, almost completely useless from the standpoint of trying to understand or change the local dynamics of pollution that affect you".
- Crowdsourcing this data is an entirely innocent scientific activity yet is profoundly radical, too.
- Javaun Moradi, product manager for NPR Digital, clarifies, "These networks aren't trying to replace scientific and government detection equipment, they're trying to both fill a data gap and advance conversation".

Q5) List and explain five critical requirements observed in Fisher's original definition for a sensor commons project.

- Fisher's original definition observed five critical requirements for a sensor commons project.
- It must:
- ▪ **Gain trust:**
- Trust is largely about the way that an activist project handles itself beyond the seemingly neutral measurements; understanding local issues, being sensitive about the ways that the sensor network itself affects the environment, engaging the public with accessible and readable information about the project, and dealing with the local authorities to get access to the systems the project wants to measure.
- ▪ **Become dispersible:**
- Becoming dispersible means spreading the sensors throughout the community.
- Getting mass adoption will be easier if the proposed sensors are inexpensive and if the community already trusts the project.
- If the sensors are complicated to set up or require massive lengths of cabling, they will get much less take-up!
- The Xively air-quality project led to the creation of the "air-quality egg", a simple, inexpensive sensor with precisely these features.
- ▪ **Be highly visible:**
- Being visible involves explaining why the project's sensors are occupying a public space.
- Being honest and visible about the sensor will help to engender trust in the project and also advertise and explain the project further.
- Advertising not just the sensors but the *data* (both online and in real life) and the ways that data has helped shape behaviour will also generate a positive feedback loop.
- ▪ **Be entirely open:**
- Being open is perhaps what distinguishes the sensor commons from a government project the most.
- Government data sets are often entirely closed, but the data that *is* released from them will be given a lot of attention because of the rigour and precision that their sensor projects will have.
- A community sensor network may have uncalibrated devices—that is, the readings for a device may be consistently out from the "correct" value and may have additional noise at the extremes of the scale.

- The openness makes up for this because all the facts about the devices and the possible errors are admitted upfront and can be improved by anyone in the community.
- ▪ **Be upgradable:**
- Finally, the project should be designed to be upgradable, to enable the network to remain useful as the needs change or hardware gets to the end of its working life.
- This requirement interplays with the dispersibility and openness of the project, and the up-front thought to managing the project long term will feed back into the trust in the project.

Q6)Which things affect more to the ENVIRONMENT and how to measure environmental cost ?

- The classic environmental concerns about the production and running of the *Thing* itself.
- **PHYSICAL THING**
- Creating the object has a carbon cost, which may come from the raw materials used, the processes used to shape them into the shell, the packing materials, and the energy required to ship them from the manufacturing plant to the customer. It's easier than ever to add up the cost of these emissions: for example, using the ameeConnect API (www.amee.com/ pages/api), you can find emissions data and carbon costs for the life-cycle use of different plastics you might use for 3D printing or injection moulding.
- You may need to consider other environmental factors, such as emissions produced during normal operation or during disposal of the object.
- For example, thermal printer paper may contain Bisphenol-A, which has health and environmental concerns.
- **ELECTRONICS**
- The electronics contained in a Thing have their own environmental cost.
- Buying PCBs locally or from a foreign manufacturer affects the carbon cost of shipping the completed units.
- If your product needs to conform to RoHS legislation, then every single component that could be extracted from it must be RoHS compliant.
- More worryingly, many electronic components rely on "rare earth minerals" (REMs) which have been extracted in China or from other locations worldwide.
- The mining process must be managed properly; otherwise, slurries formed of mildly radioactive waste minerals will be left behind long after the mines cease production. Refining them involves the use of toxic acids.
- Shipping the raw material from mine to refinery to manufacturer has its own carbon cost too.
- **INTERNET SERVICE**
- As Nicholas Negroponte (founder of MIT's Media Lab) preaches, "Move bits, not atoms".
- In the digital world, moving data rather than physical objects is faster, is safer, and has a lower environmental cost.
- Of course, "data" doesn't exist in the abstract.
- The stone tablets, and libraries of paper books that have historically been used to store analogue data always had their own environmental cost.
- Now, running the Internet has a cost: the electricity to run the routers and the DNS lookups, plus establishing the infrastructure—laying cabling across the sea, setting up microwave or satellite links, and so on.
- As well as the cost of transferring the data across the Internet, running your own web server uses power.

Q7)Explain use of THE INTERNET OF THINGS AS PART OF THE SOLUTION.

- Gavin Starks, former CEO of amee, has spoken convincingly of instrumenting the world precisely to *save* it.
- While Starks's lectures are timely and necessary, as a good hacker, he prefers to *do* something about the problem: try to solve it through technology, information, and awareness.
- We already discussed distributed sensor networks as a social and political act: the potential for global environmental action is also massive.
- If community-led sensor networks can help supplement government and international science measurements, then we should be doing everything we can to help.
- Instrumenting production lines, home energy usage, transport costs, building energy efficiency, and all other sources of efficiency might seem extreme, but it may be a vital, imperative task.
- Other technologies which aren't principally linked with the Internet of Things will also be important.
- If 67 percent of the world's water usage is in agriculture, then are there ways to reduce that quantity through technology?
- Instrumenting the supply chains, measuring to be certain that new methods really *are* more efficient, and reducing inefficiencies by automation could well use Internet of Things solutions to help measure and implement the solutions.
- The Internet of Things could become a core part of the solution to our potentially massive environmental problems.
- Projects such as a carbon score for every company in the UK will help change attitudes, perhaps simply by gamifying the process of improving one's emissions, but also by having an objective measure that could, in future, be as important to a company's success as its credit score.
- In the face of these suggestions—collective sensor networks and massive business process engineering not for profit but for environmental benefits—you might wonder whether these calls to action amount to critiques of capitalism.
- As resources become ever scarcer, a greater percentage of income might be spent on covering rental of all goods—cars, food, possibly even housing.
- The Internet of Things will also, if we let it, become a platform for whatever people want it to be.

Q8) What is CAUTIOUS OPTIMISM?

- Technology *did* change the world that they knew, for the worse, in many senses.
- But without the changes that disrupted and spoilt one world, we wouldn't have arrived at a world, our world, where magical objects can speak to us, to each other, and to vastly powerful machine intelligences over the Internet.
- As a massively interdisciplinary field, practitioners of Internet of Things may have an opportunity (or perhaps responsibility) to contribute to providing moral leadership in many of the upcoming ethical challenges.
- we should remember an important lesson on humility from Laura James's keynote at the OpenIoT assembly:
- *[Don't assume you know it all.*
- *The [I]nternet of [T]hings is interdisciplinary and it stretches most of the individual disciplines too.*
- *You will need help from others.*
- *Be ready to partner with other organisations, collaborate with people from very different backgrounds to you.]*

- When designing the Internet of Things, or perhaps when designing *anything*, you have to remember two contrasting points:
- ▪ **Everyone is not you.**
- Though you might not personally care about privacy or flood levels caused by global warming, they may be critical concerns for other people in different situations.
- ▪ **You are not special.**
- If something matters to you, then perhaps it matters to other people too.

Q9) Explain THE OPEN INTERNET OF THINGS DEFINITION.

- The Open IoT Assembly 2012 culminated in the drafting of the "Open Internet of Things Definition".
- An emergent document, created after two days of open discussion, it seeks to define and codify the points of interest around the technology of the Internet of Things and to underscore its potential to "deliver value, meaning, insight, and fun".
- A particularly interesting consensus in the definition was that, even though the Data Licensor (usually the person who has set up the sensor or paid for that data) should quite reasonably own the data from that sensor, some rights should also apply to individuals whose data is recorded (the Data Subjects).
- They *must* be granted licence to any data that regards them and *should* be allowed to license the anonymised aggregate data for their own purposes.
- We can summarize the main goals of the definition as follows:
- ▪ **Accessibility of data:**
- As a stated goal, all open data feeds should have an API which is free to use, both monetarily and unrestricted by proprietary technologies with no alternative open source implementation.
- ▪ **Preservation of privacy:**
- The Data Subjects should know what data will be collected about them and be able to decide to consent or not to that data collection.
- **Transparency of process:**
- Data Subjects should be made aware of their rights—for example, the fact that the data has a licence—and that they are able to grant or withdraw consent.
- In addition, where the data is collected from a *public* space, the public should get a right to participate in decision making and governance of that data.

- The importance placed by these principles on data is unsurprising: the Internet of Things brings the gathering and collation of data into the everyday world and has real consequences on individual privacy and power.