6. Internet - Looking forward

> "Free expression is the base of human rights, the root of human nature and the mother of truth. To kill free speech is to insult human rights, to stifle human nature and to suppress truth"
>
> *Liu Xiaobo, Nobel Peace Prize laureate of 2010 and human rights activist*

CHECKLIST FACT SHEET 23 – INTERNET OF THINGS

In the same manner that you already protect your computer and other devices from security intrusions, be sure to apply those measures to your "Internet of things" devices.

Be aware that it is difficult to protect every individual device, but that you can protect your network and reduce your areas of vulnerability.

Carefully consider any "Internet of toys" items that you plan on introducing into your home and to your child. Check the security and privacy parameters of the toy and ask yourself: "How necessary is this toy?"

CHECKLIST FACT SHEET 24 – ARTIFICIAL INTELLIGENCE, AUTOMATION AND DISRUPTIVE TECHNOLOGIES

Have you informed yourself about the latest developments in artificial intelligence and automation?

Have you invested in your interpersonal, social and emotional skills?

Have you set up your "smart" devices to ensure appropriate levels of security and user-protection?

CHECKLIST FACT SHEET 25 – VIRTUAL AND AUGMENTED REALITY

Have you talked with your child/student about key topics such as sexism, sexuality, racism, bullying, stereotypes and other forms of discrimination?

Have you made sure that the devices your child/student uses are set up correctly, with high privacy and security protection?

Have you checked that your child/student maintains a healthy life balance when using virtual or augmented technology?

CHECKLIST FACT SHEET 26 – ARE YOU THE PRODUCT? BIG DATA, DATA MINING AND PRIVACY

Have you taken the time to review the way your private data is treated by the online services you use, and to set up adequate privacy settings?

Have you recently reviewed the content you have posted online to make sure that it is still accurate and that you are still willing to share it?

Do you stay informed about the latest developments in "big data" to understand how these changes may affect you and what you can do about it?

Fact sheet 23

Internet of things

The technological advances evidenced by the recent development of Internet and wireless connectivity to data-enabled devices are causing excitement in many areas. This budding field of development known as the "Internet of things" (IoT) where web-connected devices enhance company efficiency and lifestyle convenience may also cause huge concern to parents and individuals alike.

Concerns about security, privacy and data collection are just a few issues that experts and policy makers are trying to address as more and more devices are being designed and sold. However, the IoT presents a special challenge in that experts and policy makers must find unique ways to promote the benefits of this new technology while restricting and even reducing the risks.

Not only do consumers start to ponder when "things start to think", but they must also worry about hackers accessing their "things". Read this recent article "Hackers remotely kill a jeep on a highway"[1] where two hackers remotely play with air conditioning, radio and windshield wipers,

1. http://web.archive.org/web/20160703222843/https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

before cutting the engine on a vehicle. The actions of the two hackers have sparked debate on digital security for cars and trucks.

Another area of debate is the idea that the IoT is the next industrial revolution. Today there are an estimated 10 billion connected devices, but estimated growth of this new trend in the market is expected to hit between 26 billion and 30 billion devices by 2020, with an estimated market worth of between US$6 trillion and US$9 trillion[2] .

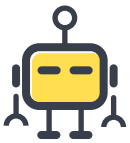
This will lead to an explosion in connected devices and a corresponding explosion in data. The General Data Protection Regulation will face new challenges in protecting privacy, when data is ubiquitous.

INTERNET OF THINGS

- The term "Internet of things" first emerged in 1999, but it was not until several years later that we saw the real existence of Internet-connected objects.
- The IoT[3] is the network of physical objects or things embedded with electronics, software, sensors and connectivity to enable them to collect and exchange data.
- The IoT is used to describe everything from intelligent thermostats that turn up the heating before you get home to refrigerators that order orange juice when you have run out. People are wearing health and fitness trackers and animals are being fitted with health and location trackers[4].
- The IoT simply means Internet connectivity where devices can talk to each other, making it easier to control and automate tasks – and collect data.
- The Pew Research Center believes that the IoT and "wearables" will have widespread and beneficial effects[5] by 2025.

WEARABLE TECHNOLOGY

- "Wearable technology" or "wearables" are clothing and accessories incorporating computer and advanced electronic technologies.
- Wearables are also called fashionable technology, wearable devices, tech togs or fashion electronics[6].
- Wearables provide instant data to the user and the user is able to instantly monitor the technology, download it for later use or send a printout.



INTERNET OF TOYS

- The IoT can also be applied to toys for children. Wireless connectivity will allow a toy to interact with other data-enabled devices or other toys.
- The Internet of toys is presenting new ways to introduce young people to technology and often encourages them to interact with the toy.
- Hello Barbie, a Mattel Internet of toys venture created in 2015 where Barbie can listen to children, caused concern for parents and privacy experts, as well as leading psychologists, who wonder if these types of toys would cause developmental issues for children, affecting their ability to create, imagine and learn autonomously. ToyTalk, a 2011 company, offers a different opinion and argues that talking toys and Wi-Fi enabled toys can offer learning opportunities to children[7].

2. https://securityintelligence.com/data-protection-in-the-internet-of-things/
3. https://en.wikipedia.org/wiki/Internet_of_Things
4. http://web.archive.org/web/20160310125239/http://www.theguardian.com/technology/2015/mar/30/internet-of-things-convenience-price-privacy-security
5. http://www.pewinternet.org/files/2014/05/PIP_Internet-of-things_0514142.pdf
6. https://en.wikipedia.org/wiki/Wearable_technology
7. http://web.archive.org/web/20150604014333/http://www.nytimes.com/2015/03/29/technology/a-wi-fi-barbie-doll-with-the-soul-of-siri.html?_r=0

- Despite the convenience offered by the Internet of things and wearables, and despite the diversion and fun offered by the Internet of toys, users may not be sufficiently aware that IoT and toy devices, just like smartphones and computers, may pose security and privacy risks. In the case of toys, there may perhaps even be child-development risks.

IMPORTANCE OF UNDERSTANDING THE ISSUES

The IoT includes wearable devices that many users may not consider as a "computing device"; as such they risk ignoring privacy issues.

The techno-futurist visions of the IoT and wearables are attractive to many. However, the entry-level positioning of the IoT means that more research needs to be done. As cybersecurity firms have learned in the past, people with criminal intent are working harder and faster to create new ways to achieve their end goal.

The advance of toy companies into the domain of the IoT means fantastic new toys for young people, but parents need to understand the risks of having open microphone devices in the hands of young people and open data links in their own homes.

ETHICAL CONSIDERATIONS AND RISKS

The ultimate goal of the IoT is to increase efficiency, but the interconnectivity that accompanies this increased efficiency may pose considerable risks.

- The idea that people can remotely access your devices and your data is a frightening prospect.
- The majority of devices and wearables are not designed with optimal security or privacy in mind.
- Recent intrusions showed hackers viewing people in their homes via baby monitors and webcams[8].
- Consumers may be as "at-risk" of cyber-intrusion as they used to be of physical intrusion in their homes.
- Consumers will need to be aware that the General Data Protection Regulation gives them control over their data and they should inform themselves about how this will work in practice.

HOW TO

- IoT devices vary in design and function. The most important instruction in the proper usage of the device is to read the instructions and to understand the functionalities of the device.
- It is necessary to go through the settings functions in order to disable or enable proper settings that afford privacy where you want it.
- Consider doing research on the device before purchase as some wearables have been recalled or do not function as marketed.
- Remember that this is a developing field and, if you wait a few weeks or months, there is always something newer, better and often less expensive on the market.

IDEAS FOR CLASSROOM WORK

- Have students create a list of all the possible devices that could be connected in a home. Then ask them to list potential security or privacy risks. What can the user do to reduce the risks? What can the device provider do? What can the Internet service provider do?

8. http://web.archive.org/web/20160406200102/http://www.bbc.com/news/technology-30121159

- After a discussion on the IoT, ask the students to draft potential instructions to consumers to help consumers understand security issues.
- Read a summary of the General Data Protection Regulation and ask the students to list all the clauses pertinent to the IoT[9].
- Download the video clip on the consumer rights awareness campaign[10] and engage the students in a discussion about consumer rights and the IoT.
- Ask young people to "develop" new toys for the Internet of toys. What are the benefits of the toy? What are the risks? How can they protect young users? How can they reassure parents that the toy is safe?

GOOD PRACTICE

It is important to be open to embracing this new technology, but you should be sure to take appropriate security measures to protect your data and your privacy.

- Restrict personal information on data-enabled devices.
- Reinforce your security on your home wireless network.
- Select strong passwords.
- Where possible, keep certain devices separate from each other.
- Limit Internet of toy interactions with your other devices, and be sure to monitor their capabilities.

Consumers must be attentive to several issues when selecting an IoT device:

- Compatibility and interoperability: is the device compatible with devices from other manufacturers or do you need to stay in the same "ecosystem" to be able to use the device? This is extremely important, as otherwise you will be "locked in" with that manufacturer with no way to switch or integrate other devices from other manufacturers.
- Connectivity: does the IoT device rely only on Internet connectivity to function properly? Ideally, you should be able to access the device without having to connect to the Internet. This is especially important as, if your device manufacturer closes down the online platform for accessing your device, it will effectively become useless.

FURTHER INFORMATION

- More information on EU "Consumer rights and law" can be found at: *<http://ec.europa.eu/consumers/consumer_rights/index_en.htm>*.
- The Guardian has reported on the Internet of things: *<http://www.theguardian.com/technology/internet-of-things>*.
- More information on the Internet of things can be found on Intel's infographic: *<www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html>*.
- Disney has carried out research on the Internet of toys: *<http://www.disneyresearch.com/project/calipso-internet-of-things/>*.
- An Internet of toys guide can be found at: *<http://www.mutualmobile.com/posts/iot-internet-toys>*.
- There is also detailed information from the Children's Digital Media Center: *<http://cdmc.georgetown.edu/publications-and-papers/textbooks/>*.
- Relevant Council of Europe documents: "Human rights for Internet users – Children and young people" *<http://www.coe.int/en/web/internet-users-rights/children-and-young-people)>*.

9. <http://ec.europa.eu/justice/data-protection/reform/index_en.htm>
10. <http://ec.europa.eu/justice/newsroom/consumer-marketing/events/140317_en.htm>