CHAPTER 5

IS THE INTERNET OF THINGS TRANSFORMING A SURVEILLANCE TOOL?

Yeşim GÜÇDEMİR[1], Kemal GÜNAY[2]

[1]Professor, Istanbul University, Communication, Public Relations, Istanbul, Turkey
e-mail: yesimgucdemir@hotmail.com

[2]PhD, Istanbul University, Communication, Public Relations, Istanbul, Turkey
e-mail: kemalgnay@gmail.com

DOI: 10.26650/B/SS07.2021.002.05

ABSTRACT

Technological development is the most important driving factor in the creation of new surveillance. The Internet of Things (IoT) has created the new surveillance term. The Internet of Things records and transmits large amounts of data which is being shared and analyzed in new and unprecedented ways to ensure the ubiquitous surveillance of individuals. This massive volume of data is called Big Data. The mass storage and accumulation of data makes it possible to monitor the lives of individuals. The IoT devices' transmissions and the amount of data are increasing rapidly day by day. All these data are available for using perpetual surveillance. These data can be used for any government, commercial, legal issue. The data gathered from the Internet of Things provides an opportunity to surveil. Governments' and companies' surveillance tools have more access than ever in human history. This has revealed the concept of big data and has caused many different challenges in terms of personal privacy too. The IoT has been used in different areas, such as automation, health, building and home automation, transportation, textile industry and public services and so on. While it offers influential and efficient solutions to challenges of humanity, the surveillance aspect of it has always been questioned.

Keywords: Surveillance, big data, technology, industry 4.0, the internet of things

1. Introduction

Surveillance is used as a control mechanism and power device by governments and it is a means of disciplining societies. In other words; supervision aims to have information about the objects being monitored and to supervise and control them in this way. A relationship of power is produced between the observer and the supervised or the continuation of the existing power relationship is ensured by surveillance. Throughout history, it has been observed that governments try to keep societies under control with different surveillance techniques in pre-modern political structures. Surveillance is now expanding as a practice of power aimed at mental and psychological power to supervise and control.

Surveillance was particularly relevant to Jeremy Bentham's book of the Panopticon, written in the 18th century. According to Bentham, surveillance is a new method of achieving mental power over the mind (Mattelart, 2012, p. 13). Observing in The Panopticon is invisible so that the object being monitored is driven to self-control, to keep its behavior under control, assuming that it is observed everywhere at any time. The minds of individuals through auto control are kept under control. Another highlight of The Panopticon is that a small number of people can easily monitor a large number of individuals in this way. This case, as Foucault points out in his "The Birth of the Prison" book (1992), has an invisible existence that can exist anywhere, anytime, and transforms into an observer that sees, hears and controls everything. According to Foucault, the model of the Panopticon is of paramount importance to understand the emergence of self-disciplined modern societies (Lyon & Bauman, 2013, p. 58).

In our globalized world, there is no need to use physical force on people anymore. The development and diversification of informatics and communication technologies are becoming a part of everyday life. All of the daily life practices are now carried into a virtual environment and every stage of social life is systematically recorded. In a digital environment, the governments take their social control and surveillance powers to the highest levels through various methods. As new technologies become widespread, the need in this way decreases. Probably in the forthcoming period, the contradiction between freedom and surveillance will create new syntheses by feeding each other mutually.

2. Surveillance

Surveillance is growing in the digital world. Today, technological change is the most significant driving factor in modern societies. Security is a political priority in many countries today and is, of course, a great source of motivation in the world of surveillance.

The prominent means of procuring security, it seems, are new surveillance techniques and technologies, which are supposed to guard us, not against distinct dangers, but against rather more shadowy and shapeless risks (Lyon & Bauman, 2013, p. 87).

Surveillance is used as a control mechanism and power device by the governments. Surveillance is a way for governments to discipline societies. In other words; surveillance aims to have information about the objects being supervised and to supervise and control them in this way. A relationship of power is produced between the surveillance and the observer and the continuity of the existing power relationship is ensured. Surveillance, defined as the "collection and analysis of information about populations in order to govern their activities" (Haggerty & Ericson, 2005, p. 3), has been the most vital tool for governments to manipulate the masses in the historical process. Throughout history, it has been seen that governments try to keep societies under control through different surveillance techniques.

Z. Bauman's state that, "Every and any kind and instance of surveillance serves the same purpose: spotting the targets, location of targets and/or focusing on targets – all functional differentiation starts from that common ground." Security points at the entrances of large places, calculating bank loans according to the credit score of the person, and checking people at the crossing points of the country are the same surveillance (Lyon & Bauman, 2013, pp. 80–81). In fact, in order to go to countries like the United Kingdom, police security systems have been moved to aircraft boarding points. The criminal status can be checked at the flight points, before boarding plane.

The last half of the 20th century has seen a significant increase in the use of technology for the discovery of personal information. Examples include video and audio surveillance, goggles, electronic tagging, biometric access devices, DNA analysis, computer monitoring including email and web usage and the use of computer techniques such as expert systems, matching and profiling, data mining, mapping, network analysis and simulation. We are a surveillance society. The general view is that we live in a time of revolutionary change with respect to the crossing of personal and social borders. New surveillance, relative to traditional surveillance, has low visibility or is invisible. It is more likely to be involuntary. Data collection is more likely to be automated involving machines rather than involving humans. Data collection is often integrated into a routine activity. It is more likely to involve manipulation than direct coercion (Marx, 2002). In the capitalist system, new surveillance tools such as IoT have further strengthened the powers of the state and capital groups. Both public and private life in society are threatened by surveillance. Every stage of life is recorded continuously with surveillance tools.

Scholars from an increasingly wide range of disciplines are discussing surveillance. For example, Bentham and Foucault offer architectural theories of surveillance, where surveillance is often physical and spatial, involving centralised mechanisms of watching over subjects. Panoptic structures function as architectures of power, not only directly but also through (self) disciplining of the watched subjects. The Panopticon has become particularly famous through Foucault's concept of panopticism, resulting in Bentham often being understood through the reading of Foucault (Galič, Timan, & Koops, 2017). In particular, Jeremy Bentham's book of the 18th-century Panopticon is related to surveillance. It is a new method of achieving mental power over the mind. Observing in panopticon is invisible so that the object being monitored is driven to self-control, to keep its behavior under control, assuming that it is observed everywhere at any time. The minds of individuals, through auto control, are kept under control. Another highlight of the panopticon is that a small number of people can easily monitor a large number of individuals in this way. This situation, as Foucault in his book, The Birth of Prison (1992), has an invisible existence that exists in every place of power at any moment and transforms into an observer that sees, hears and controls everything. According to Foucault, the model of Panopticon is very important to understand the emergence of self-disciplined modern societies (Lyon & Bauman, 2013, p. 58). As previously mentioned, Bentham's panoptic prison design (1995) is the focus of Foucault's panoptic theory (1991). This suggests that a subject will self-discipline themselves when under the pressure of a watcher. Within the prison example, this would take the form of a central guard tower which can view all prison cells around it. Prisoners would not, however, be able to see into the central guard tower. Therefore, prisoners are unsure if they are specifically being watched at any one moment. This would then mean, according to Foucault, that they would constantly self-discipline themselves on the off chance that they are being watched at that one moment. The prison cells are therefore the sole site of surveillance. Ultimately, therefore, the panopticon is centred around exercising power over a citizen's body without necessarily using force (Champion, 2019). Deleuze, Haggerty and Ericson, and Zuboff develop different theoretical frameworks than panopticism to conceptualise the power play involved in networked surveillance. This view offers infrastructural theories of surveillance, where surveillance is networked and relies primarily on digital rather than physical technologies. It involves distributed forms of watching over people, with increasing distance to the watched and often dealing with data doubles rather than physical persons. Deleuze observed that Foucauldian institutions and their ways of disciplining no longer existed, or at least were shifting into other modes of surveillance and exercising power. Deleuze, partly in collaboration with Guattari, further developed the shift, already described to some extent by Foucault, from disciplinary societies towards societies of control (Galič et al., 2017).

The above-mentioned theorists working on this subject, surveillance theories, branches out to conceptualise surveillance through concepts such as dataveillance, access control, social sorting, peer-to-peer surveillance and resistance.

Marx classified surveillance into traditional and new surveillance in his article, called "What's New About the New Surveillance". Table 1 indicates several dimensions for categorizing aspects of surveillance. He intended this comparison to make a more systematic contrast in surveillance technologies, focus on fundamental changes in modern technologies for the collection and analysis of personal information, specify the change between periods, settings and methods that the theory should take into account, provide a more logical basis for ethical and policy decisions about specific tactics and practices (Marx, 2002). Table 1 underlines differences between new surveillance and traditional surveillance.

Table 1. Surveillance Dimensions (Marx, 2002)

Dimension	**A. Traditional Surveillance**	**B. The New Surveillance**
Senses	unaided senses	extends senses
Visibility (of the actual collection, who does it, where, on whose behalf)	Visible	less visible or invisible
Consent	lower proportion involuntary	higher proportion involuntary
Cost (per unit of data)	Expensive	inexpensive
Location of data collectors/ analyzers	on scene	remote
Ethos	harder (more coercive)	softer (less coercive)
Integration	data collection as a separate activity	data collection folded into routine activity
Data collector	human, animal	machine (wholly or partly automated)
Data resides	with the collector, stays local	with 3rd. parties, often migratea
Timing	single point or intermittent	continuous (omnipresent)
Time period	present	past, present, future
Data availability	frequent time lags	real-time availability
Availability of technology	disproportionately available to elites	more democratized, some forms widely available
The object of data collection	Individual	individual, categories of interest
Comprehensiveness	single measure	multiple measures
Context	contextual	acontextual
Depth	less intensive	more intensive
Breadth	less extensive	more extensive
The ratio of self to surveillant knowledge	higher (what the surveillant knows, the subject probably knows as well)	lower (surveillant knows things the subject doesn't)
Identifiability of object of surveillance	emphasis on known individuals	emphasis also on anonymous individuals, masses
Emphasis on	individuals	individual, networks systems
Realism	direct representation	direct and simulation

Form	single media (likely or narrative or numerical)	multiple media (including video and/or audio)
Who collects data	specialists	specialists, role dispersal, self-monitoring
Data analysis	more difficult to organize the store, retrieve, analyze	easier to organize, store, retrieve, analyze
Data merging	discrete non-combinable data (whether because of different format or location)	easy to combine visual, auditory, text, numerical data
Data communication	more difficult to send, receive	easier to send, receive

2.1. Big Data Surveillance

The big data notion was first used in the Proceedings of the 8th Conference on Visualization held in 1997 by NASA researchers Michael Cox and David Ellsworth. The article is called "Application- Controlled Demand Paging for Out-of-core Visualization". In this study, it was mentioned that the data sets were massive and even the computer system's memory, disks and even external disks were filled, and this problem was called big data (Aktan, 2019).

With the advancement of technology and the development of the internet, the power of knowledge has become prominent. Humanity and machines generate massive data every second on the internet, this makes it very important to extract meaningful data. Big Data is a meaningful and processable form of all these data from different sources such as social media shares, photo archives, and cookies. Tons of data are generated daily from different sources such as social media shares, social networking, IoT devices' transmissions and the amount of data is increasing rapidly. This has revealed the concept of big data and has caused many different challenges in terms of personal privacy too.

Periods of intensive technological innovations bring an unpredictable series of side effects. The age of big data is no exception. Not only do algorithms formalize the way we feel, think, behave, and live; but also the availability of massive amounts of digital data shapes the production of scientific knowledge in many directions (Christin, 2016). Healthcare, education, journalism, finance, criminal justice etc., these kinds of expert fields are transformed in multiple ways via algorithms. Work practices, models, norms, and identities of professional actors have been changing by algorithms (Christin, 2016).

The internet has given people unprecedented access to information. It provides a massive infrastructure for connection and data-gathering. The critical science of big data must pay attention to wide transformations in communication and social organizations which create the condition where big data is suitable not just to states and corporations, but researchers too (Couldry, 2017).

Big data is a notion that defines heterogeneous data in various volumes, which cannot be processed using traditional database techniques, and consists of various digital contents (Gahi et al., 2016).

1. Structured data: Structured data refers to all kinds of data that are easy to model, input, store, query, process and visualize. In general, it is indicated in pre-defined fields with certain types and sizes, managed in relational databases or spreadsheets. In this type of data, which has a solid structure, it is easier to obtain useful information because the processes do not require high-performance capabilities or parallel techniques.

2. Semi-structured data: Semi-structured or self-describing data reflects a structured data type, but it does not just follow a solid model. In other words, semi-structured data also includes various metadata models, such as labels and signs, used to describe specific elements and hierarchical representation of different fields in the data, as well as the models in which structurality is defined. The most well-known examples of semi-structured data include XML (Extensible Markup Language) and JSON (JavaScript Object Notation) programming languages.

3. Unstructured data: Non-structural data are types of records submitted and stored except for a defined format. Usually, it consists of texts in free formats such as books, articles, documents, e-mails, and media files such as pictures, audios and videos. The fact that it is hard to present this type of data rigidly has resulted in new mechanisms such as NoSQL in the data processing processes.

Big data consists of five dimensions. These are volume, variety, velocity, veracity and value. Volume refers to the quantity of data (i.e. size of data). Variety refers to types of data (i.e. structured data, semi-structured data and unstructured data). Velocity refers to the speed with which data is generated, processed and transferred. Veracity indicates the accuracy and reliability of data. Value shows the achievement of data aggregation, analysis and the quantifiable progress that the aggregation and analysis of data provided (Gandomi & Haider, 2015).

Big data is a type of surveillance for states and companies. A great variety of organizations from healthcare to finance to law enforcement have used big data to increase their efficiency, performance and predictions (Christin, 2016). The surveillance process is similar to the big data process. It comprises gathering data, recording, and splitting it into categories in terms of people and their behaviors. A vast number of scholars underline the expanding pervasiveness of surveillance, referring to the rise of "mass surveillance", Lyon called this term "surveillance society". Big data is being exploited for surveillance practices in a great number of institutional domains beyond policing and justice, including but not restricted to health, finance, banking, credit, insurance marketing, education, immigration, defence, and activism (Brayne, 2017).

The Internet of Things extends from small household appliances to smart cities. Data on communication between smart devices is called big data. The meaning of the data used on the internet of objects is very valuable for the future. Big data enables new forms of classification and prediction using machine learning algorithms.

3. Technological Trends and IoT

The Internet of Things (IoT) is a term used to define the next-generation of internet network generated via intelligent objects with sensors and software, activated in a wide variety of fields, for instance automotive, construction, health, textile, education and transportation (Aydos, Vural, & Tekerek, 2019). Another definition of IoT is the connection of everyday objects to the internet such as television, home appliances and so on. It enables real-time and distant monitoring, a massive collection of data about people, animals, property, plants (Maras, 2015).

The Internet of Things (IoT) has become the transformation technology for many areas by creating design innovation with new digital and intelligent manufacturing technologies. Within the scope of the supply chain, the internet of objects has a wide range of applications to industrial automation, health, building and home automation, transportation and public services.

Three major industrial revolutions have taken place up to the present period. The Industrial Revolution (Industry 1.0), which started with steam engines in the 18th century and increased in production in the industrial sense, was followed by the Second Industrial Revolution (Industry 2.0), which emerged as a transition to mass production at the beginning of the 20th century and opened the way for the utilization of electricity. The mass production of goods has become standard practice (Howard, 2018). Afterwards, The Third Industrial Revolution (Industry 3.0), in which the production systems are no longer analogue, and where digital systems are used in industry, arose. In this way, the first three industrial revolutions brought mechanization, electricity and information technology (IT) to human production. These three industrial revolutions led to increased productivity in production. However, production companies in the world have faced very serious difficulties due to environmental, social, economic and technological developments at those times. To overcome these challenges, companies have always been in search of virtual and physical structures that allow close collaboration and rapid adaptation throughout the entire life cycle from innovation to production and distribution. The trade boundaries between the post-cold war countries have disappeared and purchases have started to increase among these countries. In the 1960s, customers were only purchasing the product. In the 2000s, with the involvement of the customers' requests and expectations, the service processes of the companies have become more complex. Thus, companies have now felt the need for interdisciplinary work and the Fourth Industrial Revolution (Industry 4.0), where all objects are communicated and interacted on the Internet, have emerged (Yıldız, 2018). The development of these industrial revolutions is shown in the figure below.

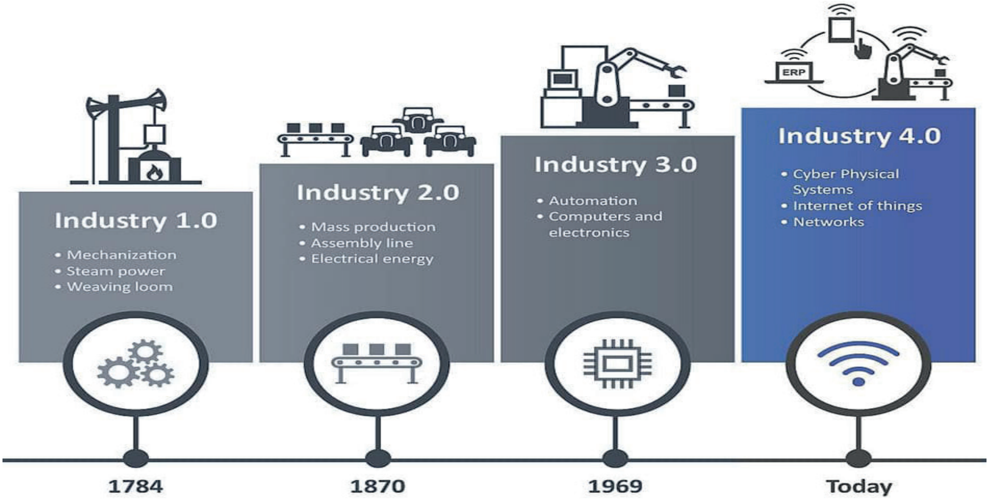


Figure 1. The History of Industrial Revolutions (Liubomyr (El.) Kachur, 2018)

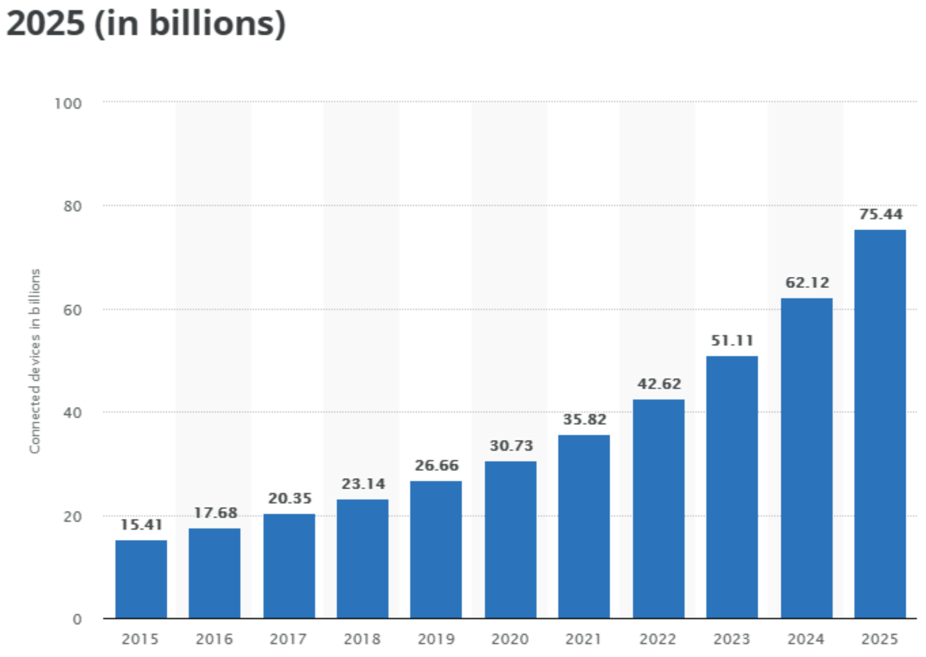
Smart objects and networks are used in every aspect of our lives in modern societies. The Internet of things positively affects human life due to the fact that many devices communicate with each other and exchange data. The Internet of Things is a technological ecosystem where devices that connect to each other interact with a network through communication protocols. IoT devices interact with each other, can process data, generate a product and work on it (Gokalp & Aydin, 2018). The Internet of Things defines the network of devices that are connected via the Internet. Being connected, such smart devices, which include smart home devices such as smart meters and smart locks, are able to share data with each other, providing benefits such as a better quality of life and greater insight into the business. The next-generation mobile connection technology 5G, with a forecasted number of 1.3

billion subscriptions by 2023, would be a major boost for the application of IoT in everyday life (Statista, 2019).

The Internet of Things is a paradigm that connects smart devices via the Internet, controlling data and conducting the application process as desired. Although the areas of application of the internet of things, which have remote sensing, performance monitoring tasks, are limited in some areas, they are exposed to applications in industry, energy systems, home automation, logistics, health, agriculture.

The Internet of Things notion was defined by Kevin Ashton during his 1999 speech for Procter & Gamble. He mentioned that Radio Frequency Identification (RFID) was a presupposition for the Internet of Things. He also concluded if whole devices were tagged, the computers system could manage, track and inventory them. To a certain extent, the tagging of things has been provided by way of technologies as digital watermarking, barcodes, and QR codes. The control of inventory is one of the more evidential edges of the Internet of things (Foote, 2016).

A very rapid increase of IoT devices has been recorded in the past few years and this ascent shows a tendency to continue. It is estimated that by the end of 2020 there will be approximately 20 billion connected devices (Mendez Mena, Papapanagiotou, & Yang, 2018). Statista indicates that the number of the Internet of Things' devices will have reached 75.44 billion by 2025 as Graph 1 below shows, a fivefold increase in decades (Statista, 2019). According to another piece of research shown in Figure 3, approximately 50 billion devices are expected to be connected to the Internet as of 2020 (Aydos et al., 2019).


2025 (in billions)

Graph 1. IoT: number of connected devices worldwide 2012-2025 (Statista, 2019)

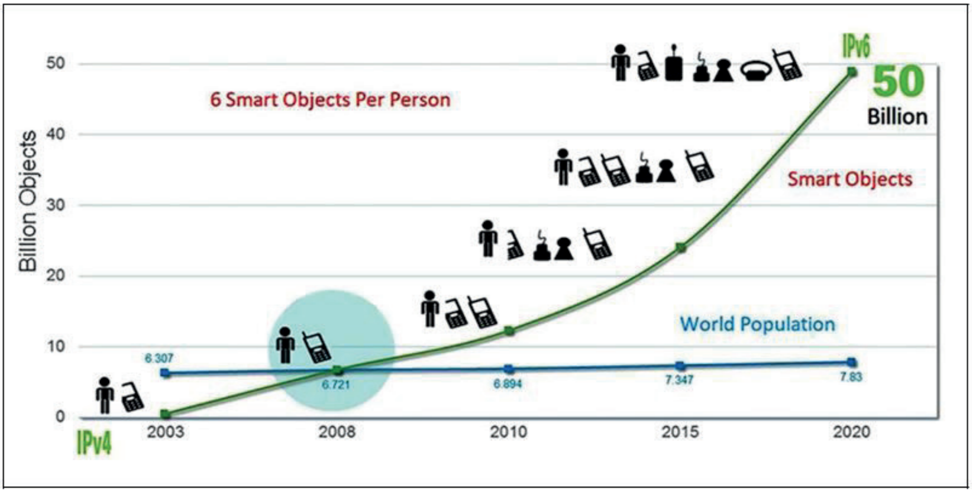


Figure 2. IoT growth chart for years

3.1. IoT and Surveillance

The mass storage and accumulation of data make it possible to monitor the lives of individuals. IoT technology makes it easy to record and collect large amounts of data, thus it ensures that people's habits and routines are better defined than ever before. This mass observation puts some pressure on people (Maras & Wandt, 2019). IoT includes efficient smart systems that can decide and implement not only data collection and use but also large data analysis methods using human-free M2M (machine to machine) interaction when needed. Besides, machines that communicate in real-time through sensors on IoT platforms enable the optimization of industrial production processes using resources efficiently and effectively (Aydos et al., 2019).

The Internet of Things is a much wider concept than simply connecting electronic devices to the Internet. IoT has the ability to communicate with people to update status information. Products developed under the concept of IoT works effectively with mobile devices. Even if users are away from their devices, devices can be controlled and managed.

IoT devices are able to use sensors such as various microcontrollers to record and transmit a large set of data. The sensors can inventory a wide variety of observable measurements (see Table 2 below). Many sensors are cost-effective, causing manufacturers to connect multiple sensors to IoT devices (Maras & Wandt, 2019).

Table 2. Examples of IoT devices and components

Sensor	**What it provides**	**iPhone X**	**iPhone 5**	**Galaxy S9**	**Apple Watch**	**My Friend Cayla Doll**	**Samsung Smart TV 9000 Series**	**Samsung Smart Dishwasher Series**
Microphone	Transmit audio within a room	X	X	X	X	X	X	
Camera	Transmit audio within a room	X	X	X	X	X		
Barometer	Measures atmospheric pressure	X		X				
Thermometer	Measures air temperature			X				X
Three-axis gyroscope	Measures orientation angular velocity	X	X	X	X	X		
Accelerometer	Measures acceleration	X	X	X	X	X		
Proximity Sensor	Detects the presence of nearby objects without the need physical contact	X		X	X	X	X	

Ambient light Sensor	Measures the amount of ambient light around the phone	X	X	X	X	X	X	X
802.11 WiFi	Communication using 802.11 WiFi protocols	X	X	X	X	X	X	X
NFC	Short-range device communication	X		X	X			
Bluetooth	Low energy device-to-device	X	X	X	X			
GPS location	Triangulates your exact location on earth	X						
Heart rate	Measures the user’s heart rate				X			

Figure 2 visualizes the use of many IoT applications for the use of people, vehicles, houses, cities, trade and industry. As is seen, computers, smartphones, school services, smart office, smart health, smart school services, smart sockets, smart grids and wearable materials are some of the Internet of Things applications. The common attribute of IoT applications is that data collection from smart objects with embedded sensors is gathered and used over the network. The Internet of Things applications are rising gradually, expanding the areas of usage and making life easier for people. A numerous amount of customized data gathered by convenient IoT applications covering smart environments, smart cities, smart metering, smart farming, smart livestock, security and emergency, retail sales, logistics, and smart health are being shared and analyzed (Aydos et al., 2019).

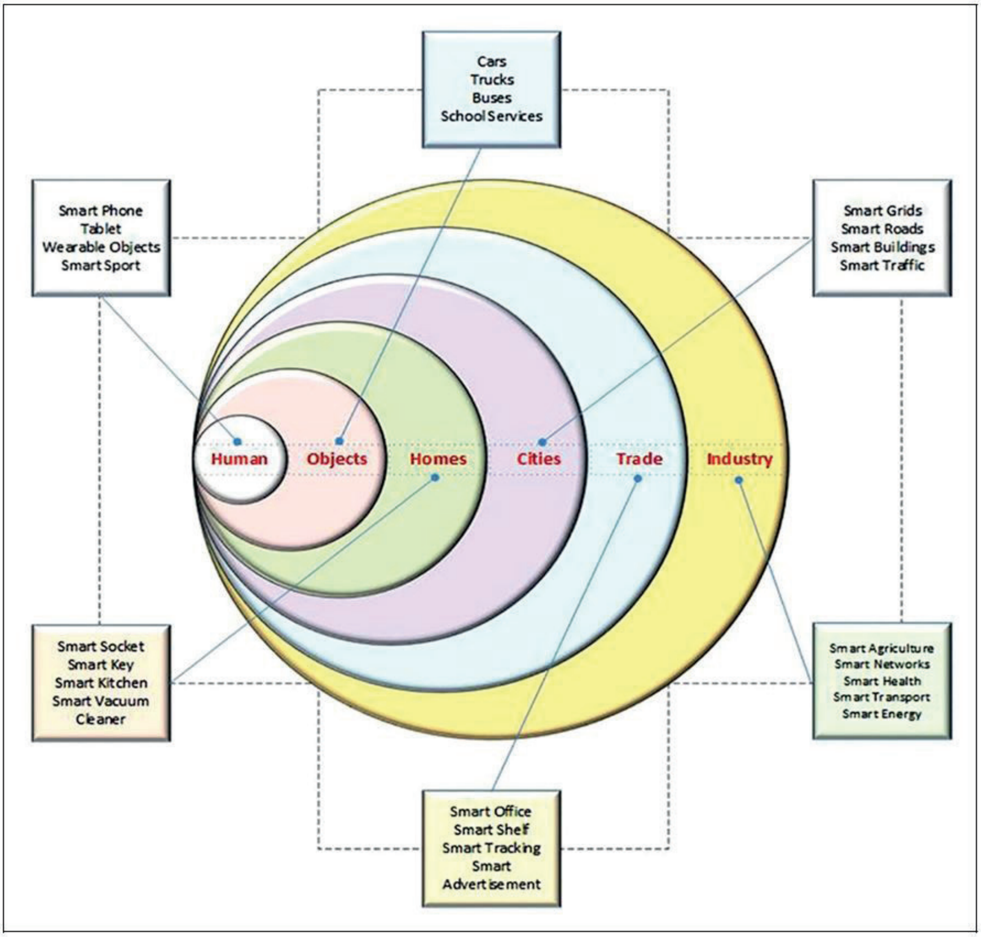


Figure 3. IoT applications (Aydos et al., 2019)

Online retail giant Amazon uses a system that not only monitors the productivity of warehouse employees but also automatically creates paperwork to fire them because they do not meet expectations. Amazon's system follows a metric called "time off task", which means workers have to stop or take a break. Previously, it was reported by The Verge that some employees felt under pressure because they did not give bathroom breaks. Amazon fulfilment centre workers face challenging conditions. The workers are forced to "make rate" with bundling hundreds of boxes per hour and lose their jobs if they don't move fast enough (Bort, 2019).

The report also indicates a profoundly automated tracking and termination process. Amazon's system tracks the rates of each individual associate's productivity. According to the document, these automation systems generate any notification of terminations regarding quality or productivity without advice from supervisors. The workers are treated like robots because they are monitored and supervised by these automated systems (Lecher, 2019). Wearable devices will be able to extract highly sensitive and personal data from employees. It is a reasonable expectation that most people are worried about surrendering such data (Weston, 2015). While it appears to be an effective measure for employers, this can become a problem and cause a drop in employee morale through monitoring. Being under constant surveillance, even at the workplace, is a controversial issue in terms of ethics and privacy.

Another example of surveillance is smart dolls such as Hello Barbie and Cayla. These dolls are designed in such a way that children can talk, sing, play and interact with them. The smart dolls make use of speech recognition and can answer children's questions. All these features can influence the behavior of users in certain ways and can manipulate and persuade them to behave differently (Keymolen & Van der Hof, 2019). The internet of things is now combined with Robotics in various diverse fields of everyday life and is preparing a new era of the Internet of Robotics. The Internet of Robotics is at the mature stage of development and is currently facing various challenges to be solved for more applications, such as design, sensors, security and long-range communication systems and so on. The Internet of Robotics IoR is improving rapidly and has the capability to use many services from monitoring, manufacturing, security surveillance in various diverse areas (Nayyar, Puri, Nguyen & Le, 2019).

Privacy and security issues can be shown at the top of the list of legal problems that may arise with the use of robots. Robots can detect, process and record the situation around them with their sensors. Robots can enter places where people cannot and can see that people cannot. Robots can be used for surveillance by people. Robots are especially used in the areas of security, travel and marketing for surveillance. Robots can enter protected areas. A home robot can be programmed to transmit information about people living in that house. It is possible for cars to follow a route, know where to stop, know how long the driver stops, know the behavior patterns of the driver in the traffic. With the Internet of Things technology, all this data can be transferred to the cloud or elsewhere. All of these activities can cause both privacy protection and security problems (Yüksel, 2017). Robots are capable of observing with advanced sensors. This requires paying special attention to privacy issues and the security of personal data. Moreover, malicious people can access the robots through the internet connection to steal personal information.

4. Conclusion

The Internet of Things enables more gathering of enormous amounts of data from people's behaviors and their daily habits than ever before. All these data are available using perpetual surveillance. These data can be used for any government, commercial, legal issue. The data gathered from the Internet of Things provides an opportunity to surveil. Governments' and companies' surveillance tools have more access than ever in human history.

New surveillance gathers the user's profile, elicits information about people's behaviors, their choices, and buying habits. Machine learning helps in modelling and predicting human habits. All these refined data can be used by governments or companies to direct or manipulate people for their purposes and goals.

Surveillance is often ambiguous, and individuals become voluntary elements of surveillance with their consent. It builds opportunities and constraints for users. IoT offers many advantages for people such as communication, automation, control, information, monitoring what you want to track, saving time and money. Constraints imply that the people who are monitored maintain self-control, keeping their behavior and their habits under control, assuming that they are being observed everywhere, anytime. Furthermore, the IoT has some disadvantages. It has complex systems; it may cause more failure than traditional systems.

The IoT may face some challenges in the near future such as security vulnerabilities, regulatory and legal issues, the determinism of the network, lack of a common architecture and standardization, scalability, limitations of the available sensors, dense and durable off-grid power sources and so on. With the involvement of IoT technologies in all areas of life, consent has been created in society to collect data of people and machines. There are some questions arise with this consent such as who will use the collected data for what purpose and where. It is also important to answer the questions of whether these transactions will be implemented in accordance with the privacy definition, how to define and provide privacy and security definitions too. The era of the IoT has just begun, it is necessary to question the assumptions and preconceptions of this new period. The presence of smart devices in all areas of our lives is steadily increasing.

References

Aktan, E. (2019). Büyük veri: Uygulama alanları, analitiği ve güvenlik boyutu [Big data: Application areas, analytics and security dimension]. *Bilgi Yönetimi* [Information Management], *1*(1), 1–22. https://doi.org/10.33721/by.403010

Aydos, M., Vural, Y., & Tekerek, A. (2019). Assessing risks and threats with a layered approach to the Internet of Things security. *Measurement and Control, 52*(5-6), 338–353. https://doi.org/10.1177/0020294019837991

Bort, J. (2019, April 25). Amazon can automatically fire warehouse workers for “time off task” [Web page post]. Retrieved from https://www.businessinsider.com/amazon-system-automatically-fires-warehouse-workers-time-off-task-2019-4

Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review*, *82*(5), 977–1008. https://doi.org/10.1177/0003122417725865

Champion, T. (2019, April 16). Are we living in a post-panoptic society? [Web page post]. Retrieved from https://www.e-ir.info/2019/04/16/are-we-living-in-a-post-panoptic-society/

Christin, A. (2016). From daguerreotypes to algorithms. *ACM SIGCAS Computers and Society*, *46*(1), 27–32. https://doi.org/10.1145/2908216.2908220

Couldry, N. (2017). Surveillance-democracy. *Journal of Information Technology and Politics*, *14*(2), 182–188. https://doi.org/10.1080/19331681.2017.1309310

Foote, K. D. (2016, August 16). A brief history of the Internet of Things [Web page post]. Retrieved from https://www.dataversity.net/brief-history-internet-things/

Gahi, Y., Guennoun, M., & Mouftah, H. T. (2016). Big data analytics for security and privacy challenges. *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 50–53. https://doi.org/10.1109/CCAA.2016.7813688

Galič, M., Timan, T., & Koops, B.-J. (2017). Bentham, Deleuze and beyond: An overview of surveillance theories from the panopticon to participation. *Philosophy & Technology 30*, 9–37. https://doi.org/10.1007/s13347-016-0219-1

Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, *35*(2), 137–144. https://doi.org/10.1016/j.ijinfomgt.2014.10.007

Gokalp, E., & Aydin, M. A. (2018). Security of IoT. *UBMK 2018 - 3rd International Conference on Computer Science and Engineering,* 453–457. https://doi.org/10.1109/UBMK.2018.8566345

Haggerty, K., & Ericson, R. V. (2005). *The new politics of surveillance and visibility*. Toronto, Canada: University of Toronto Press.

Howard, E. (2018, September 5). The evolution of the industrial ages: Industry 1.0 to 4.0 [Web log post]. Retrieved from https://www.simio.com/blog/2018/09/05/evolution-industrial-ages-industry-1-0-4-0/

Kachur, L. (El.). (2018, May 30). Industry 4.0: The top 9 trends for 2018 [Web log post]. Retrieved from https://dzone.com/articles/industry-40-the-top-9-trends-for-2018

Keymolen, E., & Van der Hof, S. (2019). Can I still trust you, my dear doll? A philosophical and legal exploration of smart toys and trust. *Journal of Cyber Policy*, *4*(2), 143–159. https://doi.org/10.1080/23738871.2019.1586970

Lecher, C. (2019, April 25). How Amazon automatically tracks and fires warehouse workers for ‘productivity’ [Web log post]. Retrieved from https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations

Lyon, D., & Bauman, Z. (2013). *Liquid surveillance: A conversation.* Malden, MA: Polity Press.

Maras, M. H. (2015). Internet of Things: Security and privacy implications. *International Data Privacy Law*, *5*(2), 99–104. https://doi.org/10.1093/idpl/ipv004

Maras, M.-H., & Wandt, A. S. (2019). Enabling mass surveillance: Data aggregation in the age of big data and the Internet of Things. *Journal of Cyber Policy*, *4*(2), 160–177. https://doi.org/10.1080/23738871.2019.1590437

Marx, G. T. (2002). What’s new about the “new surveillance”? Classifying for change and continuity. *Surveillance and Society*, *1*(1), 9–29. https://doi.org/10.24908/ss.v1i1.3391

Mendez Mena, D., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. *Information Security Journal*, *27*(3), 162–182. https://doi.org/10.1080/19393555.2018.1458258

Nayyar, A., Puri, V., Nguyen, N. G., & Le, D. N. (2019). Smart surveillance robot for real-time monitoring and control system in environment and industrial applications. In: V. Bhateja, B. Nguyen, N. Nguyen, S. Satapathy, & D. N. Le (Eds.), *Information systems design and intelligent applications: Advances in intelligent systems and computing* (pp. 229-243). Singapore, Singapore: Springer.

Statista. (2019). IoT: Number of connected devices worldwide 2012-2025. Retrieved from https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Weston, M. (2015). Wearable surveillance – a step too far? *Strategic HR Review*, *14*(6), 214–219. https://doi.org/10.1108/shr-09-2015-0072

Yıldız, A. (2018). Endüstri 4.0 ve akıllı fabrikalar [Industry 4.0 and smart factories]. *Sakarya University Journal of Science*, *22*(2), 546–556. https://doi.org/10.16984/saufenbilder.321957

Yüksel, A. E. (2017). Robot Hukuku [Robot Law]. *Türkiye Adalet Akademisi Dergisi* [Journal of Turkey Justice Academy], *29*, 85–112.