smart cities

MDPI

Review

Ethics and Law in the Internet of Things World

Spyros G. Tzafestas

School of Electrical and Computer Engineering, National Technical University of Athens, Zographou, GRI5773 Athens, Greece; tzafesta@cs.ntua.gr

Received: 4 September 2018; Accepted: 3 October 2018; Published: 12 October 2018

Abstract: The aim of the law is to maintain social order, peace, and justice in society, whereas the aim of ethics is to provide codes of ethics and conduct that help people to decide what is wrong, and how to act and behave. Laws provide a minimum set of standards for obtaining good human behavior. Ethics often provides standards that exceed the legal minimum. Therefore, for the best behavior, both law and ethics should be respected. The Internet of Things (IoT) involves a large number of objects and humans that are connected via the Internet 'anytime' and 'anyplace' to provide homogeneous communication and contextual services. Thus, it creates a new social, economic, political, and ethical landscape that needs new enhanced legal and ethical measures for privacy protection, data security, ownership protection, trust improvement, and the development of proper standards. This survey and opinion article is concerned with the ethics and legislation of the IoT and provides an overview of the following: definition and history of the IoT; general ethical principles and theories that are available for application in the IoT; the role of governments in the IoT; regulations in the European Union (EU) and United States for the IoT' IoT characteristics that have the potential to create ethical problems; IoT ethical questions and principles; IoT security, privacy, and trust aspects; and the ethical culture of IoT-related companies.

Keywords: ethics; law; internet of things (IoT); IoT devices; privacy; security; trust; EU regulations; US regulations; ethics principles; professional ethics; ethical culture; ethical leadership

> Security must be built into the foundation of the IoT solution.
>
> **Jason Porter**
>
> Trust is the backbone of IoT, and there is no shortcut to success.
>
> **Giulio Coraggio**
>
> As a global community, we face questions about security, equity, and human rights in a digital age.
>
> We need greater cooperation to tackle challenges and mitigate risks.
>
> **Antonio GutteresUN Secretary-General**

1. Introduction: What Is the Internet of Things (IoT)?

The Internet of Things (IoT), or as otherwise called the Internet of Objects (IoO), is a new development of the Internet that has entered almost all areas of human life (business, industry, healthcare, education, etc.), and is expected to change everything in society including ourselves. The IoT can be described as things/objects in our environment being connected so as to provide homogeneous communication and contextual services. IoT involves a huge number of connections of things to things and things to humans and so it is more complex than the Internet. The term Internet of Things was coined by Kevin Ashton in 1999, initially to promote radio frequency identification (RFID).

The term ‘things’ refers to everyday objects that are readable, recognizable, localizable, and addressable via information sensing devices, and/or controllable (e.g., actuators) via the Internet [1–4]. Actually, IoT enables ‘things’ to be connected anytime (any context), any place (anywhere) with anything (any device) and anyone (anybody) using any path (any network) and any service or business, as illustrated in Figure 1.

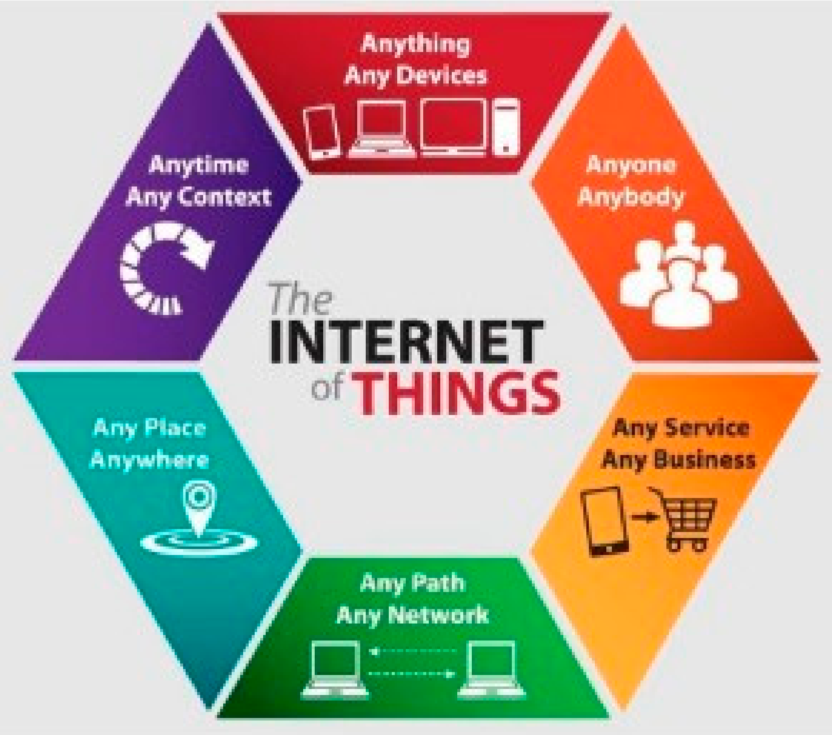

Figure 1. Internet of Things (IoT). Source: https://iottroniks.com/iot.

In IoT there are three kinds of interaction:

- People to people.
- People to things (objects, machines).
- Things/machines to things/machines.

Therefore, since IoT does not concern objects only but also interrelations between objects and humans, there is a strong need to consider the philosophical, ethical, and legal issues of IoT cohabitation with humans. The ‘principle of informed consent’ is of utmost importance in contracts between IoT providers and IoT users/consumers. Users sign before using IoT devices and services contracts with ‘terms of use’ that typically most of them do not fully understand. Very often, these terms imply that users give companies broad rights to data collection, sharing, and use. Probably, if users had comprehended the risks and harms that these terms could cause, they never would have agreed and signed them. Thus, it is of primary importance to review the IoT and understand the limitations of protective legal and regulatory frameworks, in order to provide sound recommendations for maximizing good and minimizing harm.

The range of IoT applications is continuously increasing [4,5]. Figure 2 depicts eight domains of fundamental applications. Each domain involves several distinct applications. Some other IoT applications (non-exhaustively) are: smart home, smart grids, connected cars, industrial IoT, smart supply chains, smart retail, smart banking, smart investment, smart insurance, and smart farming.

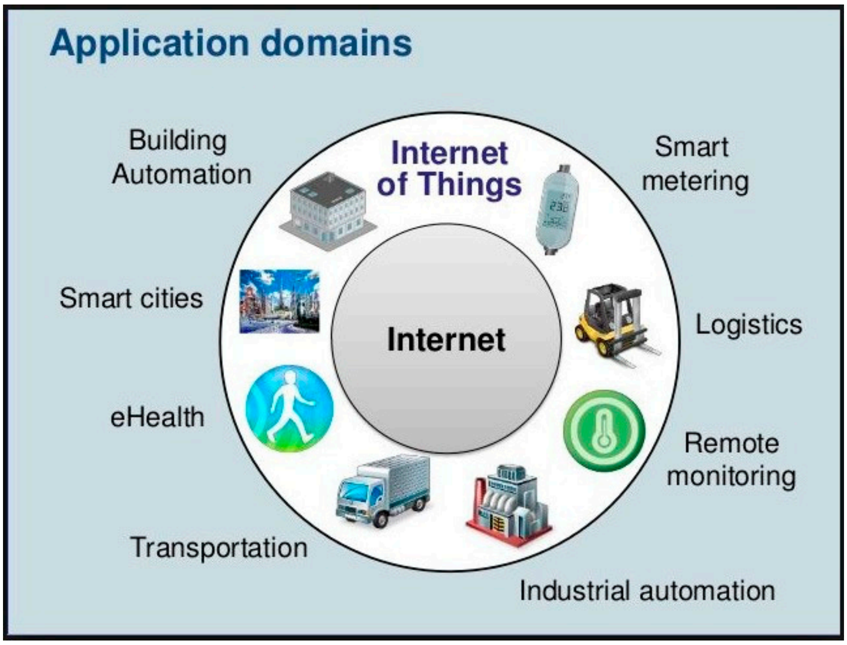

Figure 2. Eight general IoT application domains. Source: https://gr.pinterest.com/pin/654359020831382870/.

IoT devices are computing devices that connect wirelessly to a network and are capable of transmitting data. The IoT extends internet connectivity beyond standard devices (laptops, desktops, smartphones, tablets), to any type of traditionally dumb or non Internet-enabled physical devices and everyday objects. These devices, embedded with technology, can communicate and interact over the Internet, and be monitored and controlled (network controllability is a necessary feature for assuring the control of IoT devices). Much available content in the IoT has been produced using coded RFID tags and Internet protocols (IP) linked into an electronic product code (EPC) network. Large-scale IoT users need to apply 'device management' using proper management protocols, such as the Open Mobile Alliance's Device Management (OMA DM) protocol to optimize security and the operational performance of their interconnected processes during their entire life cycle. Device management should have the following features.

- Device registration.
- Device authentication/authorization.
- Device configuration.
- Device monitoring.
- Device fault diagnosis.
- Device troubleshooting.

Barriers to IoT adoption involve the following:

- Privacy and security.
- Lack of sound business structures.
- Governance structures
- Lack of interoperability.

A survey of IoT management frameworks and open challenges in IoT is provided in [6]. In particular, the software-defined networking (SDN) that has eased the management of the traditional Internet is discussed and enhanced such that it is appropriate for managing IoT. This paper, reviews past efforts for addressing issues of IoT management that involve security service provisioning, fault tolerance, energy management, and load balancing. In addition, non SDN-based approaches are reviewed.

An important class of IoT devices is that of 'wearables'. A wearable is a device that is worn on the human body and includes powerful sensors that can collect and transmit information about their environment (e.g., computerized wrist watches, Google glass, etc.). Very often, a wearable device is used for tracking vital signs about the health of the user. In [7], wearable technologies are classified in three categories:

- Wearable health technologies (for example, wearable devices that continuously monitor the health status of a patient or gather real-world information about the patient such as heart rate, blood pressure, fever, etc.).
- Wearable textile technologies (for example, clothes that can change their color on demand or based on the biological condition of the wearer or according to the wearer's emotions).
- Wearable consumer electronics (for example, wristbands, headbands, rings, smart glasses, smart watches, etc.).

Figure 3 shows a sample set of IoT wearables (Global Positioning System (GPS) position indicator, smart glasses, heart trackers, smart wrist device, smart blood pressure meter).

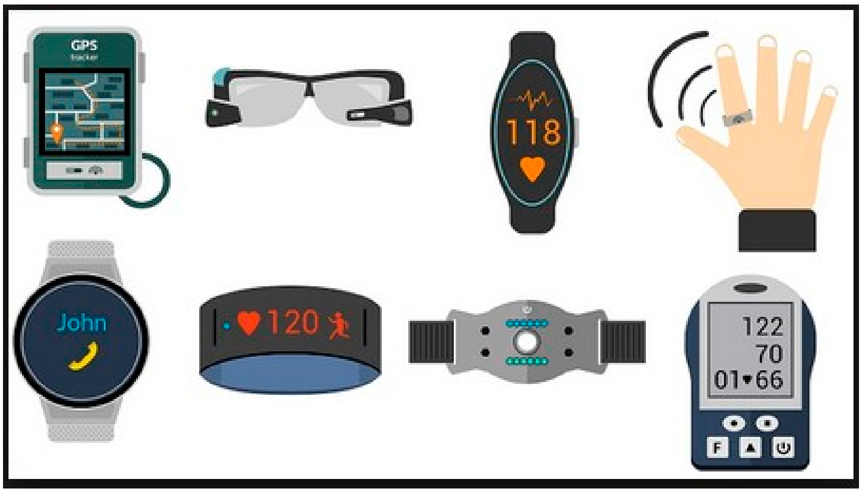

Figure 3. Examples of IoT wearables. Source https://industryresearch.company.blogspot.com/2017/10/wearable-electronics-with-iot.htm.

The purpose of this article is to discuss fundamental issues regarding the ethics and law of IoT including a brief look at the IoT, IoT history, and ethics in general. Specifically the chapter, after a short look at the question 'What is the IoT?', does the following.

- Gives a list of the key historical landmarks of IoT.
- Provides a short account of ethics (branches and methods).
- Discusses the similarities and differences of law and ethics.
- Presents fundamental general issues of IoT ethics.
- Investigates the role of governments in IoT.
- Makes a tour to the European Union (EU) and United States regulations for IoT.
- Presents the IoT characteristics that may cause ethical problems.
- Provides a list of fundamental IoT ethics questions and IoT ethics principles.
- Discusses the aspects of security, privacy, and trust in the IoT.

- Outlines the need for an ethical culture of IoT related companies, and an ethical leadership of their managers/decision makers.

2. Key Historical Landmarks of IoT

We start by listing some key historical landmarks in IoT development [8,9]. Of course there are many other landmarks in the history of the IoT that can be found in the literature.

1989: Tim Berners-Lee proposed the Internet/World Wide Web (WWW).

1991: Tim Berners-Lee created the first web page.

1998: Mark Weiser constructed a water fountain outside his office whose flow and height mimicked the volume and price trends of the stock market, and stated: "Ubiquitous computing is roughly the opposite of virtual reality, where virtual reality puts people inside a computer-generated world, ubiquitous computing forces the computer to live out here in the world with people".

1999: A big year for the IoT, a term coined by Kevin Ashton (Executive Director of the Auto-ID Center). he said: "I could be wrong but I'm fairly sure that the phrase 'Internet of Things" started life as the title of a presentation I made at Procter & Gamble in 1999".

1999: Neil Gershenfelt (MIT Media Lab): In his book *When Things Start to Think* states: "In retrospect it looks like the rapid growth of the WWW may have been just the trigger charge that is now setting off the real explosion, as things start to use the Net".

2005: UN ITU (International Telecommunications Union): publication of the report on the theme "A new dimension has been added to the world of information and communication technologies (ICTs): from any time, any place connectivity for any one, we will now have connectivity for anything. Connections will multiply and create an entirely new dynamic network of networks—an Internet of Things".

2005: Four important technologies of IoT were proposed at the WSIS: World Summit of the Information Society, namely: RFID, Nano, wireless sensors, and smart technology.

2008: First European IoT Conference: the EU recognized IoT and organized the first European IoT Conference.

2008: FCC: the FCC: Federal Communications Commission (USA) voted 5-0 to approve opening of the 'white space' spectrum.

2008: US National Intelligence Council (NIC): the NIC included IoT among the six disruptive civil technologies with potential impact on US interests up to 2025.

2011: IoT-GSI: Internet of Things Global Standards Initiative promoted a unified approach for the development of technical standards that enable IoT on a global scale.

2011: IPVC: Internet Protocol Videoconferencing (Cisco) public launch: this protocol allows for 2^{128} (about 340 undecilion) unique addresses. IBM, Cisco and Ericsson produce large educational and marketing initiatives on the topic.

2018: IoT is already mature: IoT is the third wave in the Internet-based information systems development:

- In the 1990s Internet wave 1 billion users were connected to the Internet.
- In the 2000s mobile Internet wave another 2 billion users were connected, and this number is increasing very quickly.
- Presently, the IoT has the potential to connect to the Internet as many 50 billion "things" by 2020.

3. About Ethics

The discussion on ethics that follows aims to provide a quick tour on general ethics principles and theories that are available for application in the IoT.

Ethics studies ethical behavior, investigating "what is good and bad", "what is right and wrong" and aims at the establishment and defense of rules of morality and good life (moral philosophy). Ethics belongs to "analytic philosophy" and is distinguished in [10–12] by:

- Metaethics.
- Normative ethics.
- Applied ethics.

Metaethics investigates the nature of morality, in general, and the meaning of ethical/moral judgments. Basic questions of metaethics are: "Do moral trues exist? What makes them true? "Are they absolutely true or always relative to some individual or society culture?" It seeks to comprehend the meaning of ethical properties, attitudes, statements and judgments, and how they can be supported.

Normative ethics deals with norms or set of considerations for one to act. In other words, normative ethics seeks to find what is for an action to be morally acceptable (i.e., rules and procedures for determining what a person should do or not do), and involves the theory of "social justice" (i.e., how society must be structured, and how the social goods of freedom and power should be distributed in a society). Normative ethics is also called 'prescriptive ethics' because it rests on the principles that determine whether an action is right or wrong.

Applied ethics is concerned with the application of ethics theories in actual life. Internet of Things ethics belongs to applied ethics. Applied ethics is of upmost importance to professionals in different areas of life including engineers, information scientists, doctors, managers, administrators, and so on. Ethics develops and studies the following practical ethical entities:

- Moral principles.
- Values.
- Rules and regulations.
- Rules of conduct.
- Ethical practices.

A general principle for the ethical behavior of company managers and other decision makers is expressed as: "An ethical decision is a decision that a decision maker does not hesitate to communicate outside the company because the typical person in a society would think the decision is acceptable". This is also known as: ''Front Page of the Newspaper Test':

- Would I want my decision published?

3.1. Ethics Theories

Key theories of ethics are [10,11]: virtue theory (Aristotle, Plato), deontological theory (Kant), utilitarian theory (Mill), and justice as fairness theory (Rawls).

Virtue theory: virtue ethics focuses on one's character and the virtues for determining and evaluating ethical performance. Principal advocators of virtue ethics theory are Plato, Aristotle, and Thomas Aquinas.

Virtue ethics is person- rather than action-based. It is concerned with the virtue or moral character of a human performing an action rather than with ethical duties and ethical rules, or the consequences of particular actions.

Deontological theory: the term deontology comes from the Greek words δέον (deon) meaning duty and λόγοσ (logos) meaning study. This theory was formulated and developed by Immanuel Kant and is grounded in his 'categorical imperative' proposal. It says that we are ethically obliged to act in accordance to a set of ethical principles and rules irrespectively of outcome. Deontological duties have existed and commanded by religions for many centuries before Kant, but his deontological rules (maxims) were derived from human reason.

Utilitarian theory: this theory advocates the view that an action should be morally evaluated solely on the basis of its contribution to overall utility determined by happiness or pleasure summed among all people (i.e., on the basis of its contribution to the greatest happiness of the greatest number of people or the maximum total utility for the greatest number of people). For utilitarianism, happiness and pleasure are inherently valuable, pain is inherently negatively valued, and anything else has (positive) value only if it causes happiness or prevents suffering, i.e., if it is instrumental, or a means, to an end.

Justice as fairness theory: justice as fairness was introduced by John Rawls (1921–2002) under the assumption that those who engage in social cooperation choose together in one act the principles which are to assign basic rights and duties and to determine the division of social benefits. Rawls states: 'People have to decide in advance how they are to regulate their claims against one another and what is to be the foundation of charter of their society'. In justice as fairness theory the original position of equality corresponds to the state of nature in the traditional theory of the social contract. Justice as fairness starts with the most general of all choices which people might make together, i.e., with the choice of the first principles of a conception of justice which will regulate all subsequent criticism and reform of institutions. After the choice of a conception of justice, one may suppose that they are to choose a constitution and a legislature to enact laws, and so on, all in accordance with the principles of justice initially agreed upon. In his theory, Rawls combined deontological and utilitarian theories for the evaluation of social and political bodies. The general principle of justice as fairness says:

'The general primary goods, liberty and opportunity, income and wealth, and the foundations of self-respect, are to be distributed equally unless an unequal distribution of any or all of these goods is to the advantage of the least favored'.

This principle is divided in two parts:

- Liberty principle: each human has an equal right to the widest basic liberty compatible with the liberty of others.
- Difference principle: social and economic inequalities must be regulated so as they are reasonably expected to be to everyone's benefit attached to positions and offices to all.

3.2. Other Theories

Social contract theory (Thomas Hobbes, John Locke, Jean-Jacques Rousseau, John Rawls): in this ethical system we agree to apply rules that specify how we treat others accepting the rules rationally for our mutual benefit. To formulate the rules we use the concept of 'rights' (i.e., respect the rights of others). The concept of rights is very useful and can be employed to specify what the moral domain is, or delineate the limits of government. According to social contract ethics, morality consists of the set of behavioral rules that are accepted by rational people on the condition that the other people accept them as well. Implications of social contract theory include:

- The basics (things that are necessary for the survival of any society, namely protection of life and property, protection of the society against outside threats, etc.).
- Civil rights (freedom of speech, freedom of religion, etc.).

Case-based ethics theory (casuistry): this is a modern ethics system that seeks to overcome the apparently possible divide between deontology and utilitarianism. It starts with direct immediate facts of a particular case (hence the name casuistry). Casuists begin with a particular case itself and then examine what are morally significant practical and theoretical features. The general working principle of case-based moral reasoning is grounded on the view that: 'Moral belief and knowledge evolve incrementally through reflection on cases, without essential recourse to a top-down approach'. In this belief, case-based ethical reasoning is analogous to case law ('Social ethics develops from social consensus which is then extended to new cases by analogy to past cases'). Interpretation of cases is essential for moral judgment and principles, and theories typically play a legitimate role in the interpretation.

Value-based ethics theory (J. Dewey): this ethical theory uses some value system that consists of the ordering and prioritization of ethical and ideological values that an individual or society holds. Values are categorized as:

- Ethical values that specify what is right or wrong and moral or immoral (these values define what is allowed or prohibited in the society that holds them).
- Ideological values which refer to the more general or wider areas of religion, political, social, and economic morals.

A value system must be consistent, but in real life this may not be so. Values, in general, determine either an actual or an idealized set of criteria for evaluating options, and deciding what is appropriate (economically, ethically, or otherwise), based on extensive experience. Ethical values determine what is right or wrong for both individual agents and corporate agents. To behave ethically, means to behave in a way consistent with what is right or moral. General value theory investigates 'how, why, and to what degree' humans value things of nature and life (e.g., a person, an idea, an object, etc.). This theory has its origins in ancient Greeκ philosophy under the name *αξιολογία*/axiology (φιλοσοφία των αξιών/the philosophy of values). Ethics evaluates moral entities (not physical entities or goods).

Ethics is a must for all areas of human activity, including those that fall under the umbrella of 'information' which includes the Internet/IoT area. The four ethics theories that may find profound application in the field of Internet/IoT are the utilitarian, the justice as fairness, the social contract, and the case-based theories.

4. Law versus Ethics

Law and ethics are overlapping, but ethics goes beyond law [13]. Here a comparison of law and ethics is made and their differences are pointed out.

Law: the law is defined to be the set of rules produced by the government, aiming at maintaining social order, peace and justice in society, and providing protection to the entire public and safeguarding their interests. Law is created by the judicial system of the country, and it is compulsory. Every person in the country is bound to follow the law. The law clearly specifies what a person must or must not do, and is enforced by imposing punishment or penalties or both.

Ethics: ethics is a system of moral principles which deals with what is good or bad for individuals and the society. It is a collection of fundamental concepts and principles on an ideal human character that enable people to make decisions regarding what is right or wrong. Ethics is a code of conduct agreed and adopted by people in a society, which sets the norms of how a person should live and interact with other people.

Similarities of law and ethics: laws are based on moral values and describe the basic behavior of individuals, i.e., they set the minimum standards of human (ethical) behavior. Thus, law and ethics are similar in the sense that they both are systems that maintain a set of moral values and prevent people from violating them. They both provide guidelines to people of what they may do or what they may not do in particular situations. They are both aiming at making people benefit from being members of a well-regulated society.

Differences of law and ethics: ethics is based on people's awareness of what is right and what is wrong, but laws are created and enacted by governments. Therefore, ethics may vary from people to people (because different people may have different opinions on the same issues), whereas laws describe clearly and uniquely what is legal or illegal independently of what people believe and are arguing. Violating the rules of law imply legal consequences (penalties, punishment). Violating ethical rules might involve violation of conscience, and does not imply legal consequences. An action may be legal but not ethical. The differences of law and ethics are summarized in Table 1.

Table 1. Differences of law and ethics.

Law	**Ethics**
Written formal document	Non-written principles and rules
Created by judicial systems	Presented by philosophers and professional societies
Compulsory for everyone	Personal choice (according to conscience and ethics education)
Interpreted by courts	Interpreted by each person
Priority decided by court	Priority determined by individual
Enforceable by police and courts	Not enforced but applied at will or suggested by professional societies

There are many reasons why laws are needed. These include the needs to regulate society, to protect people, to enforce rights, and to resolve conflicts. Everyone is accountable to the same laws, and these laws protect the fundamental human rights. This is the foundation of the rule of law. Laws prevent or discourage people to behave in ways that affect negatively the quality of life of other people. People, in general, follow the law. Why? There are two reasons: (i) to avoid legal consequences or sanctions (instrumental explanation); (ii) to respect the law's legitimate authority (sociological explanation). A well-known example of respecting authority from ancient Greece is that of Socrates death) [14].

5. IoT Ethics: General Issues

IoT technologies solve many real-life problems but they create serious ethical concerns and legal challenges related to:

- Protection of privacy.
- Data security.
- Data usability.
- Data user experience.
- Trust,
- Safety, etc.

Questions of ethics and responsibility in the development of IoT solutions should be addressed. IoT ethics and responsibility aspects are more complex and demanding than those of pure Internet, because of the huge amount of data generated and handled in IoT. The big question here is: "Why is it necessary or particularly important to think about ethics in IoT?" There is not a unique answer to this question. One could say, because we are going to experience a boom in the field of autonomous systems resulting in enhanced humans and smart systems, devices and organizations, all of which imply that we have to start thinking about how to bring the best of IoT rather the worst IoT. Governance and ethics are really the two keys here. Another would say, because we have to understand how to think, to design and build IoT-aided automation systems, and how to decide, in case of harm, who is responsible and who is accountable. We have to be sure of 'what does it mean to be ethical, and what does it mean to promote the public good'.

The ethics of IoT is of upmost importance both for public and private life. However, looking at the literature one can realize that only a limited number of research articles and studies of IoT ethics have been published. Here, we will outline three of them [15–17].

In ref. [15], the concept of 'Ethical Design', for the privacy problem in IoT was introduced aiming at empowering the user in the interaction with IoT. In this article the main challenges in the evolution of the Internet towards IoT were identified in order to establish interactions with the users that are respectful of their needs and privacy rights. This Ethical Design framework needs to be supported by a regulatory and standardization process, as well as by the incorporation of proper security solutions (cryptography, etc.).

In ref. [16], a number of ethical issues that may arise from the characteristics of IoT are identified and discussed. It is recognized that every individual needs to be assured that he/she is protected by effective technological solutions (encryption techniques, ID management, privacy enhancing techniques, etc.) which need to be re-interpreted and updated for IoT. It is suggested that the minimum requirements for an ethical IoT are the enforcement of the property right of information, the assurance of the access of information, the assurance of the integrity of information, and the enforcement of the right to private life.

In ref. [17], the main challenges of security, privacy, and trust for smart IoT devices are considered and the relevant literature up to 2014 is reviewed. Also a trust management framework for mobile devices is proposed by taking into account security related issues. Two major properties of trust, privacy, and security are studied, in order to propose, based on them, the objectives of trust management. For trust enhancement the paper analyzes the security requirements; access control, authentication and confidentiality. Several algorithms available in the literature for privacy preservation are also analyzed.

Other recent papers that are concerned with ethical issues in IoT include [18].

6. The Role of Governments

With IoT, governments face the responsibility of regulating the intangible entities of data and information that flows between huge amounts of sensors, devices, and networks, as information is actually the creator of value. For these different devices and sensors to be able to communicate and share data, it is necessary that they use unified standards for data structures, formats, and communication protocols. Thus, governments or other authorized bodies have to design these standards that enable them to regulate IoT. In particular, industry-wide standards for IoT, like the communication protocol standards, 4G and WiFi, or device addressing standards like IPv6, are needed. A major current issue in IoT is the lack of transparency on the part of companies about how data gathered from large numbers of users is stored and how it is used. The regulation of this issue is the responsibility of governments which should select proper criteria for data and network security. These criteria can be a good benchmark for accredited agencies to verify the security of the IoT devices and issue authoritative certificates to manufacturers of IoT devices and providers of IoT services. According to the World Economic Forum, governments need to develop and quickly master the capacity of data curation. The challenge here is that core skills and systems needed in the data age are far from the current government regulations and systems. Government organizations need to develop advanced processes and systems for big data management, and also robust processes to ensure and assure data quality. To realize such processes, governments must review a vast number of laws and regulations (enforcing privacy regulations, protecting against data-breaches regulations, regulations that ensure net-neutrality and data flows, etc.) [19]. (https://www.weforum.org/2017/02/role-of-government-digital-age-data/).

Governments play a primary role in shaping the future of the IoT. This is because governments have a double role, namely [20]:

- User role: governments plan to get smart cities all over the world and become major users of IoT. As such they set how IoT should be employed, and specify sound requirements for assuring highly secure, reliable, and robust IoT products and solutions.
- Infrastructure provider role: governments should issue regulations for devices not originally intended for connection to the IoT, as well as for devices particularly designed to be connected devices. The former class raises more crucial concerns, and the governments should release license regulations on the basis of proper security standards and compliance criteria. Governments should ensure that IoT products and solutions are used exclusively for their specified goal, otherwise there is greater risk to be compromised or to be vulnerable.

Many thinkers argue that consumer trust in IoT security can be improved through government regulations. This continuously drives IoT adoption and provides a big opportunity to companies and organizations. In [21], the replies of people to a questionnaire about the need and impact of government IoT regulations in 11 countries/areas (US, UK, France, Germany, BeNe, Middle East, India, Japan, Australia, Brazil, South Africa) are provided and analyzed.

As IoT enters all sectors of society, industry and economy, it is subject to general legislation (public law, business law, insurance law, tax law, private international/human rights law, security law, criminal law, civil liability law, consumer protection law, private/data protection law, environmental law, and so on). But, general legislation is not sufficient. Like the Internet, IoT needs more specialized legislation to address more specific situations that might occur in IoT operations. As a general rule, IoT government regulations should focus on the system capabilities (e.g., how data can be reused or sold) rather than on implementation (e.g., MySQL vs. Hadoop).

7. European Union and United States IoT Regulations

The IoT involves a huge number of connected devices via the Internet, and creates a new social, political, economic, and ethical landscape. Therefore, for a sustainable development of IoT, political and economic decision-making bodies have to develop proper regulations in order to be able to control the fair use of IoT in society. The IoT law and ethics framework should involve the following:

- Legislation/regulations.
- Ethics principles, rules and codes.
- Standards/guidelines.
- Contractual arrangements.

The regulations for IoT should include:

- Regulations for the devices connected.
- Regulations for the networks and their security.
- Regulations for the data associated with the devices.

Here, a summary of the major laws/regulations for IoT existing in the EU and USA will be provided. Most of the developed and developing countries have similar or equivalent laws.

7.1. European Union

The EU commenced activity in the IoT area in 2005 by launching "i2010: A European Information Society for Growth and Employment" that defined policies for the development of the "European Information Space" and involves innovation and investment in research and development (R&D) for including better services and better quality of life actions. Afterwards, the EU enacted the following regulations and initiatives that cover data, networks/security, and devices [20,22]:

- EU DPR-2012: European Data Protection Regulation: the purpose of this regulation [23] is to assure the protection of "personal data" of individuals independently of what type of processing is taking place. Personal data include any data than can be referred to individuals, which implies that the concept of individual data can extend to vast areas of IoT.
- EU Directive-2013/40: this Directive deals with "Cybercrime" (i.e., attacks against information systems). It provides definitions of criminal offences, and sets proper sanctions for attacks against information systems [24].
- EU NIS Directive-2016: this Network and Information Security (NIS) Directive concerns "*Cybersecurity*" issues. Its aim is to provide legal measures to assure a common overall level of cybersecurity (network/information security) in the EU, and an enhanced coordination degree among EU Members [25].
- EU Directive 2014/53: this directive is concerned with the standardization issue which is important for the joint and harmonized development of technology in the EU. Its title is: "On the harmonization of the laws of the member states relating to the marketing of radio equipment" [26].

- EU GDPR: European General Data Protection Regulation-2016: this regulation concerns privacy, ownership, and data protection and replaces EU DPR-2012. It provides a single set of rules directly applicable in the EU member states [27].
- EU Connected Communities Initiative: this initiative concerns the IoT development infrastructure, and aims to collect information from the market about existing public and private connectivity projects that seek to provide high speed broadband (more than 30 Mbps). It also attempts to identify technical assistance needs of local communities and provides targeted support to promoters of more advanced projects. The initiative brings different local communities/municipalities together in order to help them find and obtain financial support for developing business models to deliver broadband to their area [28].
- Europe 2020 "Innovation Europe" Initiative: this ambitious initiative provides a framework program for funding novel projects (IoT and other) such as the "Horizon 2020" [29]. One of the seven parts of the Europe 2020 strategy for smart, sustainable, and inclusive growth is the "Innovation Union" (IU). The IU involves several actions towards achieving the following three goals:

    1. Make Europe one of the world-class science performers.
    2. Free the innovation from obstacles such as expensive patenting, market fragmentation, and skills shortages.
    3. Revolutionize the way public and private sectors cooperate (e.g., via innovation), and enhance partnerships between European institutions, authorities (national and regional), and business.

A strong European initiative on IoT is IERC: the European Research Cluster on the Internet of Things. IERC aims among other things at [30]:

- Establishing a cooperation platform for IoT activities in Europe and becoming a major worldwide contact point for IoT research.
- Defining an international strategy for cooperation in the IoT field of research and innovation.
- Coordinating the cooperation activities with other similar EU clusters and projects on IoT and information and communication technology (ICT).
- Organizing workshops and debates leading to a deeper understanding of IoT, future Internet, 5G, and cloud technology.

IERC participants include over 50 EU-funded projects, and over 10 stakeholders of closed projects.

Another EU IoT initiative is the 'IoT European Platforms Initiative' (IoT-EPI), which funds a large number of projects covering security, privacy, data protection, and IoT trust issues, etc. One of these projects is the H2020-UNIFY-IoT Project [31], some elements of which will be discussed later.

7.2. United States

General US legislation that protects civil rights (employment, housing, privacy, information, data, etc.) includes: the Fair Housing Act (1968) [32], the Fair Credit Reporting Act (1970) [33], the Equal Employment Opportunity Act (1972) [34], the Electronic Communication Privacy Act (1986) [35], which is aplied to service providers that transmit data, the Privacy Act 1974 which is based on the Fair Information Practice Principle (FIPP) Guidelines [36], and the *Breach Notification Rule* [37] which requires companies utilizing health data to notify consumers that are affected by the occurrence of any data breach. The above legislation is general, and in principle can cover IoT activities, although it was not designed with IoT in mind. Legislation devoted particularly to IoT includes the following:

- White House Initiative 2012: the purpose of this initiative [38] is to specify a framework for protecting privacy of the consumer in a networked work. This initiative involves a report on a

‘Consumer Bill of Rights” which is based on the so-called “Fair Information Practice Principles” (FIPP). This includes two principles:

1. Respect for Context Principle (consumers have a right to claim that the collection, use, and disclose of personal data by Companies are done in ways that are compatible with the context in which consumers provide the data).
2. Individual Control Principle (consumers have a right to exert control over the personal data companies collect from them or how they use it).

- IoT Cybersecurity Improvement Act 2017: this is a bill before the US Senate that aims to improve the security of Internet-connected devices [39]. The bill defines IoT devices as any device which is connected to and uses the Internet. The bill does not put requirements on manufacturers of such devices, but it follows another approach. That is, the bill directs government agencies to include certain clauses in their contracts that demand security features for any Internet-connected devices that will be acquired by the US government. The bill describes what these clauses are and how a waiver to these required features can be obtained, and requires that the devices to be sold rely on international standards (ISO, NIST, etc.) [40].

8. IoT Characteristics that May Cause Ethical Problems

The principal IoT characteristics that potentially might cause ethical problems are the following [16,41]:

- Ubiquity/omnipresence: the IoT is everywhere. The user is attracted to IoT, absorbed by it; there is no clear way out.
- Miniaturization/invisibility: computers and devices will be smaller and smaller, and transparent, thus avoiding any inspections, audit, quality control, and accounting procedures.
- Ambiguity: the distinction between the natural objects, artifacts, and beings will be more and more difficult to be made, because the transformation from one category to another is easy, based on tags.
- Difficult identification: objects/things have an identity in order to be connected to the IoT. The access to these objects and the management of their identities might cause crucial problems of security and control in the IoT ecological world.
- Ultra connectivity: the huge number of connections of objects and people require the transfer of large quantities of data (big data) which could be maliciously used.
- Autonomous and unpredictable behavior: the interconnected objects might interfere autonomously and spontaneously in human activities in unexpected ways for the users or designers. People, artifacts, and devices will belong to the same IoT environment, thus creating hybrid systems with unpredictable behavior. The incremental development of IoT will lead to emerging behaviors that the users could not fully understand.
- Incorporated intelligence: this will make the objects as substitutes of social life. The intelligent objects will be dynamic with an emergent behavior. Being deprived of these devices will lead to problems (e.g., teenagers without the Google, smart phone or social media, might feel themselves cognitively or socially handicapped).
- Decentralized operation: the IoT control and governance cannot be centralized, because of the large number of hubs, switches, and data. The information flows will be eased, and the data transfers will be faster and cheaper, and thus not easily controllable. There will appear emerging properties and phenomena which will require monitoring and governance in an adequate way, and this will further influence the accountancy and control activities.
- A few comments on some of the above characteristics follow [16]:

- Property right on data and information: the difficulty in specifying the identification of things and humans is reflected to the difficulty to identify who is the owner of the data retrieved by IoT sensors and devices.
- Omnipresence: this makes invisible the boundaries between public and private space. People cannot know where their information ends up.
- Accessibilty of data: an attack on a PC might cause information loss. A virus or hacker attack in the IoT might have serious effects on human life (e.g., on the life of the driver of a car connected to IoT).
- Vulnerability: the list of possible vulnerabilities in IoT is scaring. It ranges from home appliances, to hospitals, traffic lights systems, food distribution networks, transportation systems, and so on.
- Digital divide: the digital divide in the IoT is enlarged. IoT operations can be understood only by experts. Communication in IoT devices affects human lives in ways that are difficult to predict or imagine. The digital divide can only be reduced by proper coherent legal and democratic frames to delineate this process.

9. IoT Ethics Questions

The greater part of IoT ethics coincides with information technology ethics and Internet ethics. Some questions, concerning the ethics of IoT, that need further consideration, are the following [42]:

- What happens if the Internet connection breaks down?
- Who is responsible or liable for patching IoT devices, routers, and cloud connections?
- Is there an assurance that hacking on the cloud side of IoT services will not have access to a home's internal network?
- What happens if an IoT service provider experiences downtime for critical life-supporting devices?
- What happens if an IoT device acts without the consent of its owner or acts in unintended ways (e.g., ordering the wrong products, or vacuuming at an unreasonable hour)?
- What happens if an IoT product vendor goes out of business and no longer supports the product?
- Who owns the data collected by IoT devices?
- Are there cases where IoT devices should not be collecting data?
- What happens if the user wants to opt out?
- What about those who do not have smart devices or the knowledge to use them? (Digital divide).

10. IoT Ethics Principles

All activities that involve the use of personal data are expected to comply with the applicable data-protection legislation. Beyond legal compliance, IoT activities should respect the ethical principles that are relevant in each particular case. A set of general ethical rules applicable to IoT activities or research projects, based on [43], is the following:

- In IoT activities, individuals should be treated as ends (not as means), and maintain their rights to property, autonomy, private life, and dignity.
- Individuals should not suffer physical or mental harm from IoT activities.
- Benefits from the application of IoT should be added to the common good.
- The necessity and proportionality of an IoT process should be taken into account and capable of being demonstrated.
- IoT applications should be performed with maximum transparency and accountability via explicit and auditable procedures.
- There should be equal access to the benefits of IoT accruing to individuals (social justice).
- IoT activities should have minimum negative impact to all facets of the natural environment.

- IoT activities should aim to lighten the adverse consequences that data processing may have on personal privacy and other personal and social values.
- Adverse effects beyond the individual (groups, communities, societies) should be avoided or minimized or mitigated.

11. IoT Security, Privacy and Trust Issues

Security: the main security domains are shown in Figure 4. The IoT consists of 'Things' and 'Applications' that exploit the features provided by 'things' [44]. IoT applications consist of data (personal data, business data, information, metadata), and algorithms (smart applications, analytics, AI/cognitive algorithms). Things consist of computing facilities (network devices, cloud computing, edge computing), and machines (wearables, sensors, robots/drones, etc.).

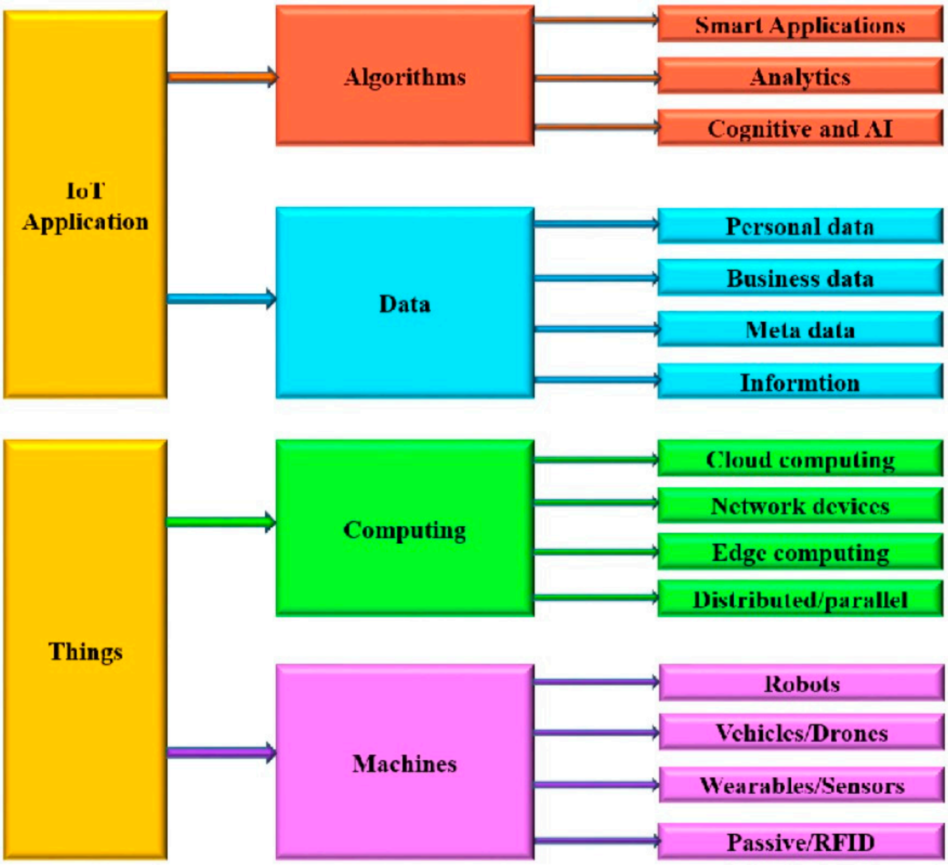

Figure 4. The IoT's security domains (needing risk analysis for trust and data protection). Source: www.unify-iot.eu/Deliverable 02.03.

Privacy: The European Union General Data Protection Regulations (EU GDPR 2016, etc.) and the equivalent US regulations impose the principles that should underlie the processing of personal information. A new principle added to EU GDPR 2016 is the principle of "Privacy by Design'. According to [44], an IoT privacy framework should include the following:

- Privacy regulations.
- Data minimization.
- Data portability.
- Transparency.
- Compliance disclosures.

- IoT engagement by default.
- IoT engagement by design.
- Best practice.

The concepts of security and privacy have many complex interrelationships, but they are not identical. A typical misconception refers to the identification of confidentiality with privacy [44]. A classification of possible relations between security and privacy was proposed by Wolfgang Hofkirchner using his 'four world views' scheme (Figure 5) [44,45]:

- Reductionism.
- Projectionism.
- Dualism.
- Dialectic.

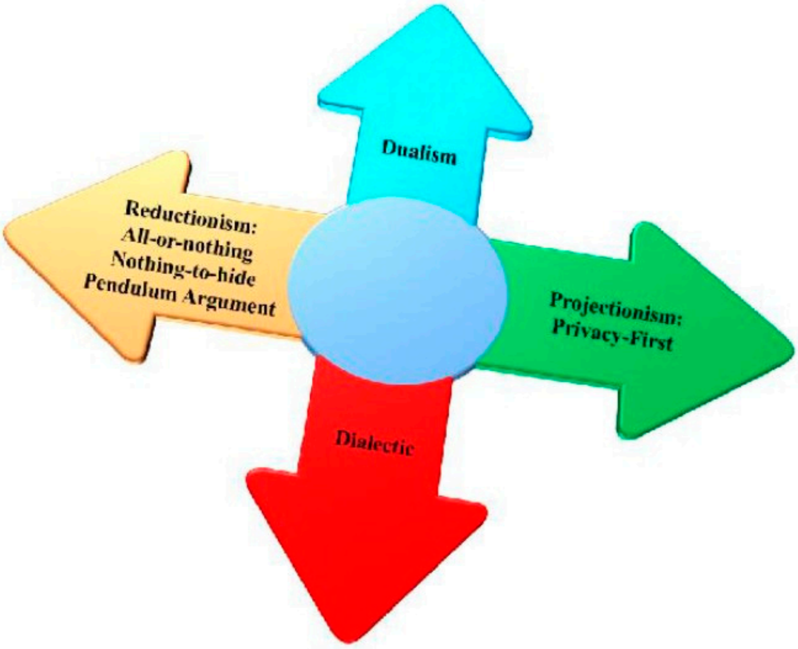

Figure 5. Privacy–security relationship: Source: www.unify-iot.eu/Deliverable 02.03.

The horizontal axis mirrors a zero-sum or mutually exclusive trade-off of security vs. privacy. The vertical axis provides alternative possibilities to the security–privacy relation [44].

According to [15,45], privacy protection should be based on the context in which the 'user' operates. Context is also important in the Internet, but in the IoT is much more important since it can change dynamically (e.g., home or office environment). Clearly, support for the context is an essential requirement of any approach aiming to address privacy aspects, and generally the relation of the IoT and user. As noted in [15], the evolution of the IoT regarding the protection of users is influenced by the following socio-legal-economic aspects and related issues:

- The trade-off between the market needs for data and correlation to support innovation, and the business success of the IoT systems and applications (public and private).
- The cost of verifying and implementing privacy enhancing technologies (PET) or other solutions for ensuring appropriate care in collection, storage, and retrieval of data.
- The accountability of IoT applications related to users' privacy.
- Support for the context where the user operates.

Trust: in general, trust can be looked-up from different views and interpretations. A trust framework should provide general principles for dealing, besides security, privacy, and safety, with the following issues [44]:

- Trustworthiness
- Dependability
- Sustainability.
- Reliability.
- Availability.
- Resilience.

Codes of ethics and codes of conduct for the IoT should contain provisions for all the above issues. Trust is fundamental in all human–human and human–technology interactions (economic, business, social, political, and so on). Providers of IoT products and services should work towards enhancing trust via proper strategies to achieve specific goals (technical/engineering goals, human-centered goals, ethical goals, etc.). Getting an IoT certificate from a qualified agency, increases trust considerably. Basic aspects that can assure high levels of trust are:

- Good reputation.
- High transparency.
- Proper education.

An IoT 'Bill of Rights', regarding data (published by Pachube, 2011) was put forward as a starting point for discussion at the 'Open Internet of Things Assembly' held in London (16–17 June 2012), and involves the following [46]:

- People own the data (or things) they create.
- People own the data someone creates about them.
- People have the right to access data gathered from public space.
- People have the right to their data in full resolution in real time.
- People have the right to access their data in a standard format.
- People have the right to delete or backup their data.
- People have the right to use and share their data however they want.

In this assembly the following Google's Working Document (Version 1.5) was presented (this is a real example of legal/ethical collection and use of data).

Core Framework

We want to build a trust network in which citizens, developers, business and cities can contribute to a sustainable data future via an open data delivery and discoverability framework.

- We believe that data generated from public space (not governed by other statutes) should be made available for use.
- We believe that customers enter relationships with vendors as independent actors, and data collected for/from/about them is available for their use, with a right action.

Agreement Principles

- Accessibility: we will publish data in an industry data format.
- Timeliness: we will release data in real-time and at full resolution.
- Privacy: we will not distribute data that contains personal identifiable information (PII) unless explicitly permitted.
- Control: we will allow the deleting and exporting of all data stored by a user.

- Licensing: users may explicitly grant legal permission for use and sharing of their data on a gradient from private to public domain."

Other areas of IoT legislature/ethics that need deep consideration include:

- Bill of Things rights.
- Bill of health data rights.
- Principles of public data.
- Principles for open government data.
- Principles for open scientific data.

12. Ethical Culture and Ethical Leadership

A strong ethical culture will motivate companies to design smarter and more inclusive products, services, and systems that avoid algorithmic deficiencies and assure global connectivity. Information/IoT scientists and engineers like other professionals (civil engineers, electrical engineers, medical doctors, managers, etc.) are able to have a great impact upon the world. They have power to act, and so they have a duty to contact that power responsibly and ethically. To formalize this need, information, internet, and computer professional organizations (ACM: Association for Computing Machinery, IEEE: Institute of Electrical and Electronics Engineers, IEE: Institution of Electrical Engineers, SIP: Society of Internet Professionals, etc.) have established codes of ethics, curriculum instructions, and accreditation requirements to enable their members to understand, appreciate, and conduct ethical behavior in their duties [47]

Codes of ethics are general and provide values and principles, and judgment guidelines, and are "empowering" and "aspirational".

Codes of conduct are specific, and provide prescriptions and directives, uniformity of behavior, and enforceable statements of specific issues.

An example of a general code of ethics with four basic values, namely responsibility, respect, fairness, and honesty, is that adopted by the Project Management Institute (PMI).

Some examples of information technology/Internet codes of ethics are the following:

- Code adopted by the Internet Architecture Board (RFC 1087).
- Code of the Society of Internet Professionals (SIP).
- Code of US Department of Health, Education, and Welfare (FIP: The Code of Fair Information Practices).
- The Declaration of the Internet Rights Charter of the Association for Progressive Communications (APC).
- Code of Computer Ethics Institute (The 10 commandments of computer ethics).

IoT-related companies (producers, service providers, distributors, etc.) should develop an ethical culture and promote ethical leadership [48,49]. Figure 6 shows pictorially the steps that a company is required to follow in order to build an ethical culture:

- Access ethics risk and opportunities.
- Develop or revise code of ethics and processes.
- Integrate ethical standards.
- Report and disclose.

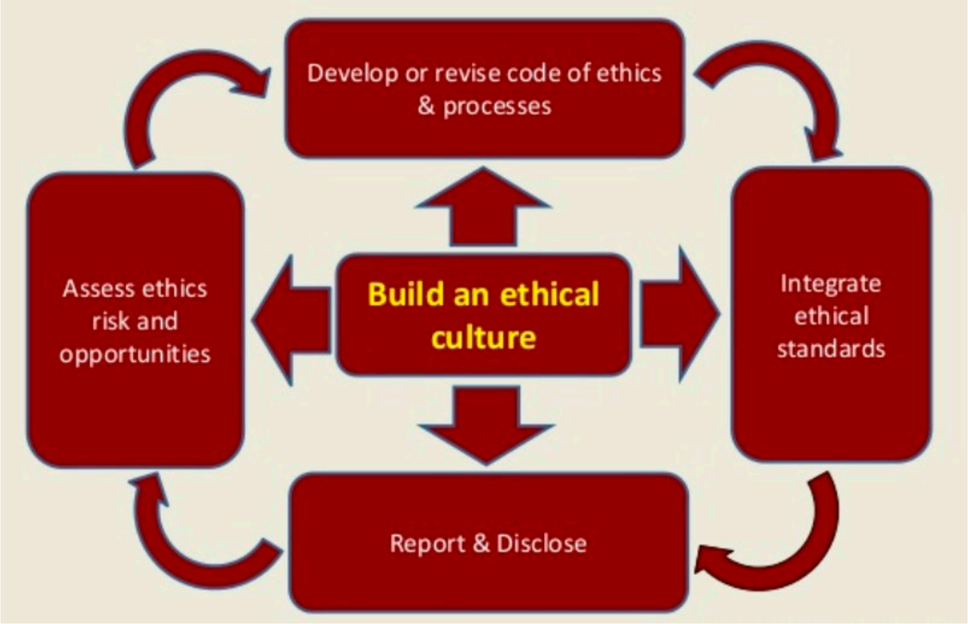
Develop or revise code of ethics & processes
Assess ethics risk and opportunities
Build an ethical culture
Integrate ethical standards
Report & Disclose

Figure 6. Algorithmic steps for building an ethical structure. Source: https://testmyprep.com/subject/ethics-and-aesthetics/codes-of-professional-ethics-reasons-for-the.

Ethical leadership is a kind of leadership in which individuals exhibit conduct for the common good that is acceptable and suitable for any type of work they perform. Ethical leadership seeks to enhance the wealth of the organization and the well-being of people via the management of ethical conduct and information. Ethical leadership is developed by respect for ethical beliefs and values, and for the dignity and rights of others. Questions that must be considered before starting the development of an organizational ethical culture include:

- How well do I understand the forces and drivers that shape an ethical culture?
- Do I know how to best interfere?
- Where can I get support to answer the above questions?

Managers can shape organizational ethical culture by: (i) performing value-based leadership; (ii) developing a formal structure system (code of ethics, disclosure mechanism, training program); and (iii) providing clear examples of strong ethical behavior. To build an ethical culture the common steps of Figure 6 should be followed.

The main characteristics of ethical leadership are: (i) demonstrates justice, (ii) manifests honesty, (iii) respects others, (iv) serves others, and (v) builds community.

According to the National Ethics Association (2012), the benefits of ethical leadership include the following:

- Reduces business liability.
- Helps employees make good decisions.
- Assures high-quality customer service.
- Prevents costly administrative errors and rework.
- Consistently grows the bottom line.

13. Concluding Remarks

The IoT is a modern IT area for research offering new important challenges both at the technological level and the human/societal level. With the IoT people can make better everyday decisions, and new services for consumers are emerging, such as pay-as-you-use, etc. Due to its heterogeneous mixture of several communications technologies, very diverse domains of application, and special features, it raises many critical legal and ethical problems that are still considerably open for further investigation, especially in the aspects of security, privacy, intellectual property rights, safety, and trust. Recent surveys across IoT-related companies and IoT users in several developed and developing countries revealed that the large majority of IoT consumers lack trust in the IoT devices and favor more government regulations to protect data access/use, privacy, and safety. These issues are becoming increasingly crucial because of the continuous expansion and penetration of the IoT in public affairs, private enterprises, and personal human life/activity. This, combined with the possible impact of 'artificial intelligence/superintelligence' in modern digital society, calls for urgent reactions on the part of the scientific community, governments, and professional societies, to quickly take proper measures or enhance existing ones to slow down and minimize negative implications. Despite peculiar ethical and legal concerns, the IoT market is growing almost exponentially as shown in the Statista Com diagram of Figure 7. In particular, according to Forbes Com forecasts, in 2018 there will be 84% growth of network connections in manufacturing [50].

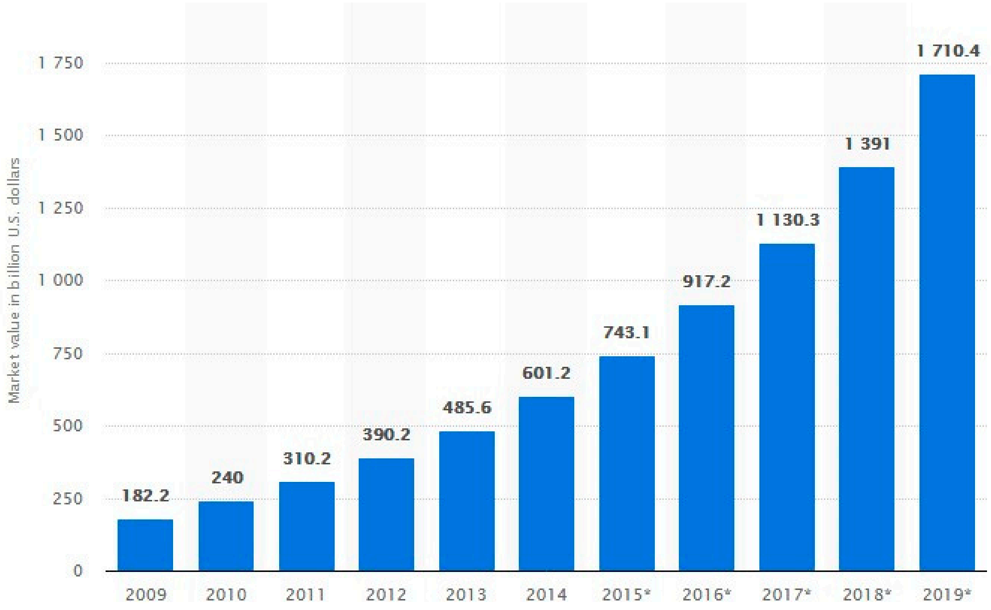

Figure 7. Growth of the IoT market from 2009 to 2019 in billion US dollars. Source: https://www.statista.com/statistics/485136/global-internet-of-things-market-size.

A branch of IoT of particular importance for the well-being of modern digital society is that of IoT-based robotics and industrial automation [51,52]. Overviews of the ethical issues related to robotics and automation are provided in [53,54]. Two important papers, worth mentioning here, are given in [55,56]. In the first, Sarah Spiekermann argues that "as we move into an era of ubiquitous computing, where the traditional Internet evolves to embrace IoT, it may be beneficial to embed an 'Idea of Man' into system design, i.e., a holistic philosophical concept that considers what Man is, what Man should be, and how Man lives with others in society". The paper explores how the Idea of Man may promote ethical system design, how it relates to technology, and how computer programmers' Idea of Man influences system design. In chapter 4 of the second paper [56], entitled "Transparency and Development: Ethical Consumption through Web 2.0 and the Internet of Things", the authors explain how the IoT can improve sourcing to create ethical supply chains. Specifically, the chapter discusses whether increased access to commodity chain information can foster progressive social and environmental change by enabling more ethical consumption. In particular, the authors examine the potential for Web 2.0 frameworks to transcend time-and-space barriers to facilitate flows of information about chains and commodities, thus encouraging consumers to make informed economic decisions by being more aware of the social, political, and environmental impacts of available commodities.

Finally, in [57], E.G. Nadhan discusses what is the real dilemma of ethics and IoT. He writes: "Humans are wired to make tough decisions bringing all context and principles to bear. Similarly can devices apply the available information to make the right judgment calls? To some extend, I would say. Will the IoT face ethical dilemmas? Absolutely. Question is, will the IoT realize it? This is the real dilemma".

Overall, the author of this article believes that 'IoT ethics and legislation' is still not sufficiently mature to cover all possible situations that might occur. More 'specific IoT legislation' and 'ethics rules for IoT' need to be developed (and frequently revised) to face sophisticated and tricky unethical and criminal behavior across the Internet/IoT. The material of this review article is presented as an inspiration towards this end. Of course, the efforts on the technological data security and safety side should be continually strengthened in order to enable efficient defense against serious hackers and invaders in the Internet/IoT world.

Funding: This research received no external funding.

Acknowledgments: The author expresses his thanks to the anonymous reviewers for their deep and constructive comments that allowed a considerable improvement of the paper's material.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. *Comput Netw.* **2010**, *54*, 2787–2805. [CrossRef]
2. Lopez Research LLC. An Introduction to the Internet of Things (IoT). Part 1 of "The IoT Series". November 2013. Available online: www.lopezresearch.com (accessed on 10 December 2017).
3. European Parliament. The Internet of Things Opportunities and Challenges. Briefing. May 2015. Available online: http://www.europarl.europa.eu/thinktank (accessed on 10 December 2017).
4. Patel, K.K.; Patel, S.M. Internet of things (IoT): Definition, characteristics, architecture, enabling technologies, application and future challenges. *Int. J. Eng. Sci. Comput.* **2016**, *6*, 6122–6131.
5. Sharma, K.; Tiwari, R. A review paper on "IoT" smart applications. *Int. J. Sci. Eng. Technol. Res.* **2016**, *5*, 472–476.
6. Kiani, F. A survey on management framework and open challenges in IoT. *Wireless Commun. Mob. Comput.* **2018**. [CrossRef]
7. Cicek, M. Wearable technologies and its future applications. *Int. J. Electr. Electron. Data Commun.* **2015**, *3*, 45–50.
8. Internet of Things (IoT) History. Available online: https://www.postscapes.com/internet-of-things-history (accessed on 10 December 2017).
9. Galipeau, D.; United Nations Social Enterprise Facility. A brief history of the IoT. In Proceedings of the APEC Philippines 2015: Workshop on IoT Development for the Promotion of Information Economy, Boracay Island, Philippines, 14 May 2015.
10. Gert, B. *Morality*; Oxford University Press: Oxford, UK, 1988.
11. Shafer-Landau, R. *The Fundamentals of Ethics*; Oxford University Press: Oxford, UK, 1988.
12. Jonsen, A.; Tulmin, S. *The Abuse of Casuistry: A History of Moral Reasoning*; The University of California Press: Los Angeles, CA, USA, 1990.
13. Hazard, G.C., Jr. Law, morals, and ethics. *South. Ill. Univ. Law J.* **1995**, *19*, 447–458. Available online: http://digitalcommons.law.yale.edu/fss_papers/2372 (accessed on 18 December 2017).
14. D'Amato, A. Obligation to Obey the Law: A Study of the Death of Socrates. *S. Cal. L. Rev.* **1975**, *49*, 1079.
15. Baldini, G.; Botterman, M.; Neisse, R.; Tallacchini, M. Ethical design in the internet of things. *Sci. Eng. Ethics* **2016**, *24*, 905–925. [CrossRef] [PubMed]

16. Popescul, D.; Georgescu, M. Internet of things: Some ethical issues. *USV Ann. Econ. Public Adm.* **2013**, *13*, 208–214.
17. Rehiman, R.; Veni, S. Security, privacy, and trust for smart mobile devices in the internet of things: A literature study. *Int. J. Adapt. Res. Comput. Eng. Technol.* **2015**, *4*, 1775–1779.
18. AboBakr, A.; Azer, M. IoT ethics challenges and legal issues. In Proceedings of the 12th International Conference on Computer Engineering and Systems (ICCES), Cairo, Egypt, 19–20 December 2017; pp. 233–237.
19. What is the role of government in the digital age? Available online: https://www.weforum.org/2017/02/role-of-government-digital-age-data/ (accessed on 28 March 2018).
20. BBVA Research Digital Economy Outlook—3. The Internet of Things: European Regulation. Available online: https://www.bbvaresearch.com/the_internet_of_things_european_regulation_DEO_Jul16-Cap3.pdf (accessed on 18 December 2017).
21. Gemalto Com. The State of IoT Security: Government Regulations and Impact. Available online: https://www2.gemalto.com/iot/iot-regulations.html (accessed on 18 December 2017).
22. Eisenhart, S. European Internet of Things Cybersecurity Recommendations: IMPACT for Medical Devices (ENISA Recommendations). Available online: https://www.emergobyul.com/blog/2017/12/european-internet-of-things-cybersecurity-recommendations-impact-medical-devices (accessed on 18 December 2017.).
23. European Commission. *Proposal for General Data Protection Regulation*; COM 11/4 Draft; European Group on Ethics in Science and New Technologies, European Union: Brussels, Belgium, 2014.
24. EUR-Lex Document 32013L0040. Directive 2013/40/EU of the European Parliament and the Council of 12 August 2013. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013L0040 (accessed on 18 December 2017).
25. NIS Directive. The Directive on Security of Network and Information Systems. Available online: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive (accessed on 18 December 2017).
26. EUR-Lex Document 32014L0053. Directive 2014/53/EU of the European Parliament and the Council of 16 April 2014. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0053 (accessed on 18 December 2017).
27. EUR-Lex Document 32016R0679. Regulation (EU) 2016/679 of the European Parliament and of the Council. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (accessed on 18 December 2017).
28. EU Connected Communities. Available online: https://ec.europa.eu/digital-single-market/events/cf/connected-communities-experience-sharing/item-display.cfm?id=15644 (accessed on 15 January 2018).
29. Europe 2020 “Innovation Europe”. Available online: http://ec.europa.eu/research/innovation-union/index_en.cfm?pg=home (accessed on 15 January 2018).
30. IERC: Internet of Things Research. Available online: www.internet-of-things-research.eu/about_ierc.htm. (accessed on 11 October 2018).
31. UNIFY-IoT. Available online: www.unify-iot.eu (accessed on 28 March 2018).
32. Fair Housing Act. 1968. Available online: https://www.justice.gov/crt/fair-housing-2 (accessed on 15 January 2018).
33. Fair Credit Reporting Act. 2012. Available online: http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf (accessed on 15 January 2018).
34. Equal Employment Opportunity Act. 1972. Available online: https://www.eeoc.gov/eeoc/history/35th/thelaw/eeo_1972.htm (accessed on 15 January 2018).
35. Electronic Communications Privacy Act. 1986. Available online: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285 (accessed on 15 January 2018).
36. Fair Information Practice Principles. Available online: http://itlaw.wikia.com/wiki/Fair_Information_Practice_Principles (accessed on 20 January 2018).
37. Breach Notification Rule (2009). Available online: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.htm (accessed on 20 January 2018).

38. White House. Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. 2012. Available online: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (accessed on 20 January 2018).
39. Internet of Things Cybersecurity Improvement Act of 2017. Available online: https://www.scribd.com/document/355269230/Internet-of-Things-Cybersecurity-Improvement-Act-of-2017 (accessed on 20 January 2018).
40. Kallis, P. The US "Internet of Things Cybersecurity Improvement Act of 2017" as an Example for EU Regulation? Available online: www.leidenlawblog.nl/activities/the-u.s.-internet-of-things-cybersecurity-improvement-act-of-2017 (accessed on 20 January 2018).
41. Van den Hoven, J. Internet of Things. Factsheet-Ethics Subgroup IoT-Version 4.01. 2012. Available online: http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation (accessed on 20 January 2018).
42. Clubb, K.; Kirch, L.; Patwa, N. The Ethics, Privacy, and Legal Issues around the Internet of Things, W231. 2015. Available online: https://www.ischool.berkeley.edu (accessed on 20 January 2018).
43. Raab, C.; Stewart, J.; Dominguez, A.; Klein, E.; Chapple, S. University of Edinburgh IoT Initiative Principles v1.1c. Available online: www.iot.ed.ac.uk (accessed on 9 May 2018).
44. UNIFY-IoT PROJECT: Policy Recommendation of the Uptake of IoT in the European Region, Deliverable 02.03. Available online: www.unify-iot.eu (accessed on 28 March 2018).
45. Nissenbaum, H. Respecting context to protect privacy: Why meaning matters. *Sci. Eng. Ethics* **2015**, *24*, 831–852. [CrossRef] [PubMed]
46. Open Internet of Things Assembly. London. 2012. Available online: https://www.postscapes.com (accessed on 28 March 2018).
47. Chadwick, R. Professional ethics. In *Routlege Encyclopedia of Philosophy*; Craig, E., Ed.; Routledge: London, UK, 1998.
48. Leigh, A. *Ethical Leadership: Creating and Sustaining an Ethical Business Culture*; Kogan Page: London, UK, 2013.
49. Starrat, R.J. *Ethical Leadership*; Wiley: New York, NY, USA, 2004.
50. PlantServicesCom. Available online: https://www.plantservices.com/industrynews/2017/forbes-releases-iot-forecasts-for-2018-notes-84-growth-of-network-connections-in-manufacturing (accessed on 28 March 2018).
51. Simoens, R.; Dragone, M.; Saffioti, A. The internet of robotic things: A review of concept, added value and applications. *Int. J. Adv. Robot. Syst.* **2018**, *15*. [CrossRef]
52. Brevold, H.P.; Sandstrom, K. Internet of things for industrial automation: Challenges and solutions. In Proceedings of the IEEE Conference on Data Science Technical Solutions and Data Intensive Systems, Sydney, NSW, Australia, 11–13 December 2015.
53. Tzafestas, S.G. Roboethics: Fundamental concepts and future prospects. *Information* **2018**, *9*, 148. [CrossRef]
54. Tzafestas, S.G. Ethics in robotics and automation: A general view. *Int. Robot. Autom. J.* **2018**, *4*, 229–234. [CrossRef]
55. Spiekerman, S. About the 'idea of man' in system design: An enlightened version of the internet of things. In *Architecting the Internet of Things*; Uckelman, D., Harrison, M., Michahelles, M., Eds.; Springer: Berlin, Germany, 2011.
56. Smith, M.L.; Reilly, K.M.A. *Open Development: Networked Innovations in International Development*; The MIT Press: Cambridge, MA, USA; IDRC: Ottawa, Canada, 2013.
57. Nadhan, E.G. The Real Dilemma of Ethics and IoT. Available online: https://www.experfy.com/blog/the-real-dilemma-of-ethics-and-iot (accessed on 11 October 2018).