The Need for a RIoT (Responsible Internet of Things): A Human Rights Perspective on IoT Systems

Prof. Luca Belli

Luca Belli, PhD is Professor of Internet Governance and Regulation at Fundação Getulio Vargas (FGV) Law School, where he heads the CyberBRICS project, and associated researcher at Centre de Droit Public Comparé of Paris 2 University. Before joining FGV, Luca worked as an agent for the Council of Europe Internet Governance Unit. Over the past decade, Luca has authored and edited more than 30 research outputs in English, French, Italian, Portuguese and Spanish, amongst which "De la gouvernance à la régulation de l'Internet" (Berger-Levrault, 2016); the "Net Neutrality Compendium" (Springer, 2016); "Platform Regulations: How Platforms are Regulated and How They Regulate Us" (FGV, 2017) and "Gobernanza y Regulaciones de Internet en América Latina" (FGV, 2018) and the "Community Network Manual" (FGV-ITU-ISOC, 2018). Luca's works have been i.a. quoted by the Organization of American States Report on Freedom of Expression and the Internet (2013); used by the CoE to elaborate the Recommendation of the Committee of Ministers on Network Neutrality (2016); featured in the French Telecoms Regulator (ARCEP) Report on the State of the Internet (2018), and published or quoted by various media outlets, includingLe Monde, BBC, The Hill, O Globo, El Pais, El Tiempo, La Vanguardia and La Stampa.

Fundação Getulio Vargas Law School, Rio de Janeiro | luca.belli@fgv.br

Introduction: The Rise of the Internet of Things (IoT)

The Internet of Things (IoT) is heralded by its proponents as a true propellant of the next industrial revolution, able to generate considerable gains in efficiency and prompt growth "at an astronomical rate."[84] The concept of IoT is quite flexible and, to date, it does not enjoy a universally agreed definition. However, the various authors conducting research on the IoT – and the distinct definitions that each of them provides – converge highlighting that the main feature of this phenomenon is the connection of the physical world, composed by all "things," with the digital world of the Internet.

The IoT can therefore be broadly defined as a network linking uniquely identified physical objects together with electronic networks and software applications enabling data collection, communication and processing. Device manufacturers and service providers generally hail the evolution towards such interconnection as enabling the rise of "smart technologies" facilitating extensively marketed phenomena such as "Smart Cities", "Smart Farming" and the "Industry 4.0", which are based on the widespread data collection and processing allowed by the exploitation of IoT systems.

In fact, the IoT already encompasses billions[85] of so-called "smart" devices around us that can be uniquely identified and are able to collect, store, process and communicate a wide range of data about their functioning and about the environment – and, therefore, also the individuals – around them. Indeed, the purpose of the IoT is facilitating the connection of all everyday objects and devices to electronic networks, which may be the Internet but also closed networks such as private intranets, in order to enhance data collection and improve efficiency through data processing.

The IoT builds upon the success of a number of technological enablers[86] that make the interconnection of billion devices possible. Due to its potential, the development of the IoT is considered with great attention by several stakeholders both from the private sector, particularly telecommunication operators, service providers and device manufacturers, and from public bodies eager to shape an IoT policy environment able to facilitate business and attract investments, while preventing, avoiding – or at least mitigating – privacy and security risks.

In this perspective, the International Telecommunication Union argues that the identification, data collection, processing and communication capabilities of the

IoT shall make "full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled."[87] Indeed, connected devices and, consequently, IoT systems are instrumental to deploy services based on increasingly fine-grained, ubiquitous and voluminous data collection and processing capabilities, likely to increase efficiencies in areas such as smart city services, public surveillance, healthcare, building management systems. The wide range of data collected and shared by the devices parts of the various IoT systems is indeed nurturing complex data processing, producing insights that allow increasing the efficiency of both processes and devices involved.

The IoT is therefore a concept comprising a growing number of technologies able to expand the reach of the Internet into the physical world, allowing to monitoring – potentially permanently and ubiquitously – both the status of the connected objects and of the surrounding environments. In this perspective, the interconnection of every object can also generate risks for the protection of personal data of the individuals adjacent to the connected things as well as for their personal security and for public safety, should the devices be hacked. Indeed, the possibility to remotely control or manipulate connected devices may lead adversely affect the enjoyment of individuals' fundamental rights, not only interfering with individuals' privacy[88] with particular regard to family life, home and correspondence, but also as regards the security of person, non-discrimination or to access information.[89] When such networks and devices are not conceived, maintained and secured in the most responsible fashion, their users as well as all peoples monitored by senders embedded in the "smart" things may suffer nefarious consequences on an ample spectrum of rights.

In this perspective, states and business enterprises that are involved in IoT systems must act in synergy, analysing risks and elaborating and implementing effective policies, regulation and adjudication, prompting a Responsible Internet of Things (RIoT), where people's privacy and security are at the centre of the new digital ecosystems. It is important to stress IoT systemically in order to understand the complexities, risks and benefits of such phenomenon and frame it responsibly.

The IoT is therefore concept comprising a growing number of technologies able to expand the reach of the Internet into the physical world, allowing to monitoring – potentially permanently and ubiquitously – both the status of the connected objects and of the surrounding environments… When such networks and devices are not conceived, maintained and secured in the most responsible fashion, their users as well as all peoples monitored by senders embedded in the "smart" things may suffer nefarious consequences on an ample spectrum of rights.

The purpose of this chapter is, therefore, to briefly investigate what technological evolutions are driving – and being enabled by – the IoT, what could be the impact of the IoT on individuals' fundamental rights and what elements could allow public and private stakeholder to comply with the United Nations Guiding Principles on Business and Human Rights (UNGPs), by building RIoT systems. In this perspective, this paper will be structured in three sections. The first section will analyse the IoT phenomenon, stressing the intimate link between the IoT and the Big Data and Artificial Intelligence phenomena. The second section will briefly scrutinise the impact that the aforementioned phenomena may have on the full enjoyment of fundamental rights, providing some concrete examples. The concluding section will provide some suggestions on how tech-businesses developing connected objects can implement the UNGPs effectively.

The Interplay between IoT, Big Data and Artificial Intelligence

According to Gartner (2014), the IoT will reach 26 billion units by 2020, up from less than a billion of connected devices in 2009, while Cisco (2016) predicts that 500 billion devices are expected to be connected to the Internet by 2030. It is therefore important to stress that IoT systems are going to be ubiquitous and pervading the offline environment where we live without living clear ways of opting out and avoid the impact pf connected objects' connectedness.

The integration between physical and digital worlds fostered by the IoT and the data collection capability it facilitates are likely to affect not only the performance of services and connected devices but also to deploy direct effects on individuals. Notably, the fact that objects are permanently connected with other objects, applications and communications networks, and that such objects can be remotely controlled directly impact individuals. Such impact does not only concern the way individuals interact with objects but also and crucially the relationships amongst people, between people and businesses as well as between people, businesses and public bodies.

Indeed, due to their undoubted potential for data collection, sharing and processing, IoT systems are deemed as an indispensable element to power data-hungry services, based on the exploitation of Big Data[90] analytics and of Artificial Intelligence[91] (AI) capabilities, which are driving the technological evolution of both public and private sector.[92]

However, it seems important to stress that, despite the hype around the IoT within technology circles, the majority of technically uneducated people may be unaware that their personal data are harvested and shared – more or less securely – by the objects that can be commonly found in the environments where they live, work or play with their children.[93] In such context, the deployment of IoT systems hold promise to confuse and deceive individuals, who may not even notice the tiny RFID tags and sensors that are embedded in connected devices, thus making it nearly impossible to perceive that everyday objects are connected to the Internet and can collect, transmit and process data about their surrounding environment.

Such ambiguity should therefore be corrected by the development of clear and effective policies, regulation and adjudication able to assist IoT developers to exercise their corporate social responsibility, while raising individuals' unawareness of the impact that IoT systems will deploy on their environment. Notably, robust data protection and cybersecurity frameworks are especially relevant to foster the sustainable development of IoT systems, avoiding that individuals are deceived and personal data are misused. This consideration becomes even more significant considering the intimate intertwinement existing between the IoT and two related phenomena, Big Dataand AI, which the IoT is supposed to nurture with a continuous flow of very diverse personal and non-personal data.

IoT solutions are already implemented in several sectors, such as connected cars, mobile health or smart metering solutions for utilities like gas or electricity, where Big Data analytics and AI are increasing deployed by a number[94] of business actors. On the one hand, Big Data analytics and AI applications are the "key enabler[s] allowing realising the full potential of the IoT"[95] as they rely on the processing of massive data datasets, bringing together data from different sources – including for example GPS location data of specific devices, social media postings, meta-data from communications, etc. – that are scrutinised algorithmically in order to find correlations. On the other hand, the data collection capabilities provided by IoT systems become instrumental to fully exploit the potential of Big Data and AI which are based on the extensive use of high volumes of varied data to improve decision-making or product and service efficiency.

To understand the correlation between the IoT and the Big Data phenomenon, it seems useful to offer two examples of how data collected and generated by a multiplicity of connected things can be combined to nurture Big Data and AI for both private and public services. A classic example is the establishment of so-called Smart City services, where data from sources such as sensors installed in public transportations and police vehicles, connected (traffic) lights and information on public events can be combined to foresee and optimise traffic flow in real time and identify the areas that are in immediate need of attention. The media and entertainment industry is also a telling example of how IoT data can enrich Big Data analytics and AI processing information collected and generated by digital platforms, such as music or video streaming services, and connected devices such as connected TVs or speakers. Indeed, such information collection and processing will allow to garner deeper understanding, infer patterns and make data-driven decisions that are becoming essential to predicting the interests of audiences, extract insights on specific groups of customers and effectively targeting them with customised advertisements for media.

However, the collection of large amounts of data, from a wide spectrum of sources and sensors may occur in the unawareness of the individuals about which data are collected by online platforms and mobile apps and, of course by connected "things." Furthermore, it is important to stress that the main criteria driving the design and implementation of Big Data analytics and AI capabilities may not be the respect of individuals' fundamental right, but rather cost minimisation and private profit maximisation. As such, IoT-powered Big Data and AI can become a tool to discriminate specific populations,[96] for instance excluding entire groups from having access to specific rights, services or opportunities, based on opaque algorithmic decisions or predictions.[97]

Importantly, the massive datasets that IoT systems hold promise to generate and the ubiquitous sensory capabilities that characterise IoT systems can not only maximise predictive intelligence but also surveillance capabilities facilitated by AI technologies, raising important privacy and security questions, while predicting and automating an increasing number of aspects of our daily lives. At its core, AI analyses and optimises data for a variety of purposes spanning from, voice-assistance, to the prediction of consumer habits, to self-driving cars or medical diagnoses. Therefore, combination of AI and IoT-generated data could be utilised to help individuals in their daily tasks, increasing productivity and improving health care but could also give rise to more dystopic scenarios, based on ubiquitous surveillance and AI-defined decisions directly implemented into the offline world of connected infrastructures and smart homes and devices.

The interconnectivity of all objects (to be) produced and AI systems or the use of IoT systems to feed Big Data analytics are therefore poised to affect every aspect of our lives and environments. Such scenario has remarkable implications for individuals' right. The following sections will identifies some of the most substantial challenges, that both public administration and business entrepreneurs need to address as urgently as possible, in order to guarantee that the development of the IoT and its interplay with Big Data and AI are a driver for positive change rather than the propellant of a dystopic future.

Human Rights Issues Raised by IoT Systems

The rise of IoT systems and the possibility that such systems continuously collect and supply data to computing technologies taking decisions over humans raises a number of public policy issues related to the IoT governance,[98] with particular regard to privacy, security, free development of personality and non-discrimination.

Data collected and generated by sensors embedded in everyday objects, such as smartphones, toys, wearable devices and urban furniture can often be precise enough to understand and predict accurately the lifestyle, commercial behaviour and other relevant patterns of entire groups of individuals or of a specific person. As pointed in the previous section, the dissemination of connected devices and the incorporation of sensors in all "things" will transform data collection into a permanent and omnipresent practice, thus giving rise to several human rights concerns.

Indeed, the range of risks to which individuals are exposed[99] in IoT environments is not limited to loss of privacy and security, enabled by connected devices permanently collecting data and, subsequently, storing, processing and transferring them in an unsecure fashion. On the contrary, such risks are conspicuously amplified, on the one hand, by the exploitation of IoT systems to feed Big Data and AI able to take decision on individuals and, on the other hand, by the possibility that such connection between computing and devices can concretely shape the physical environment where individuals' live and impact individuals physically.

Loss of individual control over personal data becomes a very likely scenario, considering that not only the permanent and automatic data-collection capabilities of connected objects but also that data collected by connected devices and sensors are often “repurposed” to be processed for a different objectives. Such objectives can be substantially dissimilar from the mere functioning of the connected “things” and processing may be executed by an organisation other than the one originally in charge of the data collection. Furthermore, the fact that connected devices can collect data automatically, rather than requesting individuals to provide such data wilfully, poses serious risks regarding individual awareness of and consent to data collection.

This is the case, for instance, of sensors in public areas or in public transportations –increasingly common in Smart City projects[100] – that capture an ample range of personal data, such as images of passersby or unique identifiers of peoples’ mobile phones.[101] This type of collection and processing is unlikely to be deemed as compliant with core data protection principles such as lawfulness, fairness and transparency[102], which are at the basis of privacy frameworks in more than 120 countries around the world. On the contrary, to respect individual’s data privacy, the entities who deploy and implement IoT systems shall make sure their data collection practices are compatible with legislation and, chiefly, that the individuals whose data are collected are duly informed as to what type of data about them is collected and for what purpose.

This scenario is particularly flagrant when data collected via IoT systems feed Big Data analytics. Although it may be argued that the purposes of Big Data analytics are frequently unknown prior to the analytics and that the interest of such analytics is precisely the capacity to reveal unexpected inferences and correlations, it is important to emphasise that this cannot be a justification to operate opaque analytics and to deceit or mislead data subjects. As such, when personal data are harvested via connected devices and utilised for Big Data, it is essential that individuals be aware that data collection is ongoing and that the secondary purpose of the analytics be compatible with the original one. As an instance, data collected through connected urban furniture to analyse and increase urban safety should not be used to profile passersby for commercial purposes such as determining the amount of their (life, health or car) insurance premiums.

In this perspective, it is useful to stress that a distinction must be stricken between the collection of data via IoT systems to power analytics whose purpose is the detection of general trends and data-collection and processing that are operated to extract inferences about individuals and make decisions affecting them. In this latter case, the mix of IoT systems and Big Data analytics may not only be incompatible with the original purposes for which data were collected by the connected devices and sensors but is also likely to create new personal data about individuals. A telling example may be the utilisation of car sensors to collect and process vast amounts of data about a given vehicle, for instance for maintenance purpose and car-performance enhancement, but also to identify patterns in the driver’s behaviour and create a profile to determine the amount of insurance premiums. In this perspective, organisations utilising data collected by IoT systems must be able to find the suitable moment where appropriate information on what data are collected and for what purpose can be provided to the affected individuals, so that they can retain meaningful choice to authorise or deny the collection and (specific types of) processing of their data.

Furthermore, it important to always keep in mind the systemic nature of the IoT to realise the interdependence of privacy and security issues. The connection of thousands or millions of diverse devices brings a proportional number of vulnerabilities and, therefore, risks that can be exploited by cyber-attackers whose level of sophistication is increasingly high. Hence, practices such as data encryption, de-identification of personal data and the implementation of strict access control mechanisms are essential to prevent unwanted dissemination of data and effectively protect the privacy of all people impacted by a specific IoT system.

With regard to the impact that IoT systems may have on security, it is important to stress the double dimension of such policy issue, encompassing both individuals’ right to security and informational security. As demonstrated by Miller and Valasek (2015), who elaborated a method to remotely took control over the brakes and accelerator of Jeep connected cars, the hacking of unsecured IoT systems may have direct consequences on individuals' lives. On the other hand, cybersecurity concerns may directly impinge upon public safety, as compromised IoT systems may allow hackers to access and remotely control public infrastructures such as connected machineries in hospitals, traffic lights, power plants etc. In this perspective, IoT security is not only essential to preserve individuals' privacy or security but also to guarantee public safety against unwanted infiltration and manipulations. Therefore, the security of all components of IoT systems must be a priority to be considered as indissociable from privacy protections, rather than a minor or optional concern for developers.

Lastly, it must be stressed the increasing interdependence between and IoT systems and the software and computing capabilities provided by AI companies. The influence of such companies on connected device developers may be explained considering the fundamental importance of software and computing power to guarantee that connected devices function smoothly. Bloomberg Technology has recently reported an example of such influence, highlighting that Alphabet (Google's parent company) and Amazon, which provide leading voice-assistance software powering a wide range of smart-home gadgets, are reported to actively ask device makers to modify the device parameters to receive continuous streams of data that can be harvested and processed by the software providers. In such scenario, smart- device users may be unknowingly[103] – and likely unwillingly – providing a wide range of information regarding the use of the smart device, regardless of whether the device being switched-on or off.[104]

Aware of the fact that connected object and sensors enable constant collection and sharing of data, it becomes essential for individual to retain knowledge and control on when and how their personal data are collected, by whom and for what purposes. Furthermore, to facilitate the secure use of connected devices, it becomes essential to utilise reliable mechanisms for authentication and authorization able to prevent unauthorized access to IoT systems and preserve data integrity.[105] Lastly, the use of data anonymisation techniques becomes increasingly important to facilitate the use and reuse of data collected via IoT systems while reducing risks connected with the loss of control over personal data.

Conclusions: Unleashing the RIoT

To maximise the benefits and reduce – and ideally eliminate – the risks determined by the emergence of IoT systems, public and private stakeholders are called to cooperate and give full force to the UNGPs. States must embark on their duty to protect individuals against human rights abuses by developing appropriate strategies, policies, regulation and adjudication mechanisms that guarantee the protection of privacy and security and clearly define boundaries so that the IoT may not be used to do harm to individuals. Corporations must meet their responsibility to respect Human Rights, acting with due diligence, assessing when IoT systems can have adverse impacts on individuals and designing products and services that prioritise the respect of individuals' rights. In addition, both public and private actors shall provide access to effective remedies, both judicial and non-judicial, for victims of any harm produced by the use of IoT systems.

Governments and business actors should jointly develop and implement IoT plans, starting by developing frameworks for risk-assessment of IoT security, categorising IoT devices according to risks and vulnerabilities and, importantly, assessing the level of dissemination in the market. Secondly, public and private actors should promote – and individuals should demand – the adoption of software best practices in all IoT devices. Such practices include privacy and security by design[106] and through the entire development lifecycle of every element composing the IoT system, as well as the possibility to "patch" and update software, manage user identity and, importantly, the existence of a permanent point of contact to signal the existence of software and hardware vulnerabilities.

Importantly, an essential element of any strategy aimed at successfully implementing the UNGPs is to seek the involvement of civil society. In this respect, the users of connected device and the public generally should play a key role in the IoT governance. Communication and education of the public are key elements and should not be seen as unilateral processes but rather as ways of mutually informing and contributing to more secure and reliable IoT systems. Information sharing regarding software and device vulnerabilities is a clear example of how multi-stakeholder cooperation is not simply useful but necessary. Indeed, the implementation of secure IoT systems requires a collaborative effort as no stakeholder alone can identify and patch vulnerabilities to secure the entire system. On the other hand, national policies – including with regard to education – are essential to raise awareness regarding the challenges of IoT. Legal frameworks must consider individual knowledge and consent to personal data collection as essential requirements, as every person shall be able to choose whether to be part of an IoT system or not and data collection and processing should never be arbitrary imposed.

Transparency should be ensured so that people are appropriately informed about the nature and the purpose of data collection and have clear and intelligible information regarding what personal data are collected about them, with whom such information is shared, as well as how to access and rectify or delete such data at any moment. To this latter extent, the development of national legal frameworks guaranteeing meaningful data privacy in an environment where the IoT, AI and Big Data are common practice should be seen as an essential element.

States should at a minimum having proper data protection framework in place, mandating to:

1. obtain consent to data collection while providing meaningful information,
2. minimise the amount of data collected to avoid potential risks and abuses,
3. guarantee that data subject enjoy the possibility to easily access,
4. rectify and delete personal data,
5. and adopt all necessary provisions to maintain personal data secure.

To comply with their responsibility to respect human rights, private sector actors should, at a very minimum:

1. make a policy commitment to the respect of human rights;
2. adopt a human rights due-diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights;
3. and have in place processes to enable the remediation of any adverse human rights impacts they cause or to which they contribute.[107]

Furthermore, innovative manners of letting individuals express their consent to (certain) types of personal data processing should also be explored, shifting the focus of data protection to a "design-thinking" approach, rather than relying on a strictly legal approach based on the classic notice and consent strategy, which has shown to have clear limits.[108] In this respect, the concept of "Data Control by Design"[109] (DCD) should be explored by policymakers, to complement the classic privacy by design approach through the implementation of appropriate technological tools putting individuals at the centre of data processing, allowing them to choose what personal data about them can be processed and for what purposes.

The DCD concept aims at expanding privacy by design, by promoting the adoption of interoperable data control tools allowing the collection of personal data, while letting the individuals defining how her data can be utilised.[110] The use of such a design thinking approach, implemented through "machine readable"[111] technological solutions, would put individuals at the centre while allowing devices and software collecting and processing data within IoT systems automatically understand and respect user choices as regards their data. Furthermore, the DCD concept may prove suitable to frame IoT systems as individuals would be able to predefine via interoperable solutions how they want their data to be collected and processed rather than having to express their consent or not to the data collection operated by every single connected object. Such dichotomy, generally proposed by data protection frameworks and based on either accepting loss of control over data in exchange of the possibility to utilise to services or denying access to data while losing the possibility to utilise services, is indeed highly inefficient as it does not allow for a more nuanced approach where individuals may chose only in certain types of processing or collection only from certain types of devices.

Lastly, when we consider the potential pervasiveness of IoT systems and the great variety of uses and potential abuses that can be done of such systems, security considerations become uppermost in the list of issues to be effectively and systemically addressed by responsible businesses and governments. Importantly, Weber (2015) points out that, since a variety of heterogeneous processes are concerned into the design, implementation and maintenance of IoT systems, the achievement of security and privacy relies on the pursuit and implementation of the four fundamental goals:

1. resilience to attacks so that the system avoids single points of failure;

2. data authentication;

3. access control on the data provided;

4. meaningful privacy, including data anonimisation, to avoid – or at least make very difficult – to extract inferences by processing personal data without the data subject consent.[112]

These goals should be pursued while keeping in mind that, in an IoT environment, everybody is vulnerable and the best way to mitigate risks is to educate individuals about their, rights, their roles and responsibilities in the digital age. It is only through collaboration and synergy that public and private actors and civil societies will be able meet the challenges presented by the IoT, maximise its benefits and avoid risks, thus unleashing a true RIoT (Responsible Internet of Things).

References

Amigo I. 8 May 2018. The Metro Stations of São Paulo That Read Your Face. Citylab. https://www.citylab.com/design/2018/05/the-metro-stations-of-sao-paulo-that-read-your-face/559811/

Angwin, J., Larson, J., Mattu S., and Kirchner, L. 23 May 2016. Machine Bias. ProPublica. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Bastone N. 20 February 2019. Google says the built-in microphone it never told Nest users about was 'never supposed to be a secret'. Business Insider. https://www.businessinsider.nl/nest-microphone-was-never-supposed-to-be-a-secret-2019-2/?international=true&r=US

Belli L., De Filippi P. and Zingales N. (Eds). (2015) Recommendations on Terms of Service & Human Rights. United Nations Internet Governance Forum. https://www.intgovforum.org/cms/documents/igf-meeting/igf-2016/830-dcpr-2015-output-document-1/file

Belli. L, Schwartz. M. Louzada L. (2017) Selling your Soul while Negotiating the Conditions: From Notice and Consent to Data Control by Design. Health and Technology Journal. 7(4), 453-467. Topical Collection on Privacy and Security of Medical Information. Springer-Nature. http://link.springer.com/content/pdf/10.1007%2Fs12553-017-0185-3.pdf

Cisco. (2016) At a Glance: Internet of Things. https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf

Day M. 12 February (2019) Your Smart Light Can Tell Amazon and Google When You Go to Bed. Bloomberg Technology. https://www.bloomberg.com/news/articles/2019-02-12/your-smart-light-can-tell-amazon-and-google-when-you-go-to-bed

European Commission. January (2013) Report on the Consultation on IoT Governance. http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1746

Gartner. 19 March 2014. Gartner says the Internet of Things will transform the data center. http://www.gartner.com/newsroom/id/2684616

Greenleaf, G. 24 May 2018. Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi, 25 May 2018. UNSW Law Research Paper No. 18-56. https://ssrn.com/abstract=318454

GSMA. December 2015. Unlocking the Value of IoT through Big Data. Version 1.0. https://www.gsma.com/iot/wp-content/uploads/2015/12/cl_iot_bigdata_11_15-004.pdf

High P. 30 October 2017. Carnegie Mellon Dean of Computer Science on the Future of AI. https://www.forbes.com/sites/peterhigh/2017/10/30/carnegie-mellon-dean-of-computer-science-on-the-future-of-ai/#4a8a2df32197

IoT Analytics. 8 August 2018. State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

ITU (International Telecommunication Union). 2012. Next Generation Networks – Frameworks and Functional Architecture Models: Overview of the Internet of Things. Series Y: global information infrastructure, internet protocol aspects and next-generation networks. Recommendation ITU-T Y.2060 (06/2012) renumbered as ITU-T Y.4000 on 2016-02-05.

ITU (International Telecommunication Union). (2005) The Internet of Things. ITU Internet Reports. Geneva: ITU.

Leswing K. 21 Oct. 2016. A massive cyberattack knocked out major websites across the internet. Business Insider. https://www.businessinsider.com/amazon-spotify-twitter-github-and-etsy-down-in-apparent-dns-attack-2016-10

Miller J. 12 August 2013. City of London calls halt to smartphone tracking bins. https://www.bbc.com/news/technology-23665490

Maddox T. 18 February 2018. Cisco: The Internet of Everything is at tipping point. TechRepublic. https://www.techrepublic.com/article/cisco-the-internet-of-everything-is-at-tipping-point/

Miller C. and Valasek C. 10 August 2015. Remote Exploitation of an Unaltered Passenger Vehicle. www.illmatics.com/Remote%20Car%20Hacking.pdf

Ng A. 5 June 2018. Amazon will stop selling connected toy filled with security issues. Cnet. https://www.cnet.com/news/amazon-will-stop-selling-connected-toy-cloud-pets-filled-with-security-issues/

O'Neil C. (2016) Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. New York: Broadway books.

Pasquale F. (2015) The Black Box Society – The Secret Algorithms That Control Money and Information. Cambridge and London: Harvard University Press.

Privacy International. 15 February 2019. The police can use IMSI catchers to track your phone, and even intercept your calls and messages. https://privacyinternational.org/feature/2729/police-can-use-imsi-catchers-track-your-phone-and-even-intercept-your-calls-and

Sicari S., Rizzardi A., Grieco L.A., Coen-Porisini A. (2015) Security, privacy and trust in Internet of Things: The road ahead. Computer Networks 76.

Weber R.H. (2015) Internet of things: Privacy issues revisited. Computer Law & Security review. 31.