Table of Contents

International Journal of Technoethics

Volume 11 • Issue 2 • July-December-2020 • ISSN: 1947-3451 • eISSN: 1947-346X

Research Articles

Book Review

Open Access Article

COPYRIGHT

The *International Journal of Technoethics* is indexed or listed in the following: ACM Digital Library; Bacon's Media Directory; Cabell's Directories; Compendex (Elsevier Engineering Index); DBLP; Google Scholar; JournalTOCs; MediaFinder; PsycINFO®; Public Affairs Information Service (PAIS International); SCOPUS; The Standard Periodical Directory; Ulrich's Periodicals Directory; Web of Science; Web of Science Emerging Sources Citation Index (ESCI)

Information Privacy and Emerging Technologies in the UAE:

Current State and Research Directions

Dimitrios Xanthidis, Higher Colleges of Technology, UAE
https://orcid.org/0000-0002-1349-5749

Christos Manolas, Ravensbourne University, UK
https://orcid.org/0000-0003-0057-8374

Ourania Koutzampasopoulou Xanthidou, University of Malaya, Greece
https://orcid.org/0000-0002-2659-7138

Han-I Wang, University of York, UK
https://orcid.org/0000-0002-3521-993X

ABSTRACT

The rapid developments of emerging technologies, including Big Data, Cloud Computing, and Internet of Things, are causing many societies to struggle whilst trying to keep up with, and adopt them. As a consequence, serious concerns and issues are being raised. The threat to personal information privacy is one of these issues. This review paper briefly introduces the aforementioned technologies and explores concepts related to concerns on information privacy and disclosure in the U.A.E. in the context of these technologies. In addition, related research themes that could be interesting to explore are identified, with a focus on the local environment.

KEYWORDS

Big Data, Cloud Computing, Information Privacy, IoT

INTRODUCTION

In Article 12 of the Universal Declaration of Human Rights, issued by the United Nations General Assembly on 10 December 1948, the right to personal privacy is recognized in the following statement:

> *No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks (National Commissions for UNESCO, 2010, Jan. 4).*

In addition to the, easier to identify, implications of the above in a broader ethical and social context, the advent of information technology and digital communications has added new concerns and issues, specifically related to information privacy. This, relatively new, concept has attracted

DOI: 10.4018/IJT.2020070101

widespread attention in the recent years, partially due to the rapid increase of the amount of information being gathered and published over the Internet.

Although the term information privacy may be difficult to define explicitly, according to Son and Kim, it "refers to an individual's ability to control when, how, and to what extent his or her personal information is communicated to others" (Son & Kim, 2008). This is also echoed on Such and Criado's view that "privacy is not just about what you reveal about yourself; it is also about what others reveal about you" (Such & Criado, 2018). At the same time, Hong and Thong (2013) approach information privacy from a more pragmatic angle by stating that it is "the privacy of personal information and usually related to personal data stored on a computer". Irrespectively of the perspective one adopts to define it, what is important to note in the context of this study is that most definitions underline the individual's right to keep personal information outside the public domain. As such, it can be claimed that this right is expected to be protected by law from unauthorized access, irrespectively of whether this relates to the physical or digital domain. In this context, it may be useful to attempt a brief distinction between the two definitions of privacy:

- Physical Privacy: The perspective that deals with the physical access to a person's property and its surroundings (H. J. Smith, Dinev, & Xu, 2011).
- Information Privacy: The perspective that addresses the access to information that can specifically identify a particular individual and may, or may not, be available online.

Between the two, it appears that most researchers and scholars are currently concerned with *information privacy*. An apparent reason for this is the mass collection of user data through online media and electronic sources. Such data collection includes, but is not limited to, customer data, student data, or public records. More specifically, while millions of users share personal information online on a daily basis, they are largely unaware of the level of access third parties have to their data, and what they do with it (Zaeem, German, & Barber, 2018). It must be noted here that most companies nowadays have rather transparent privacy policies that can be easily accessed online. However, the question of how far they are willing, or allowed, to go to collect personal data without informing their customers remains largely unanswered. Indeed, research shows an increasing public concern about how companies and authorities handle the personal data they gather (Ipsos, 2019, Jan. 25). Such concerns are also reflected in relevant statements the United Nations General Assembly Resolution and the United Nations Human Rights Committee, which on 18 December 2013 reaffirmed the right to privacy in the digital age, and demanded that "working of State Surveillance be subject to legality through clear and precise law, which law must look to safeguard the right to privacy".

In addition to the expressed positions of researchers and scholars, the above is also reflected in the views of individuals, who generally appear to be aware both of the importance of protecting their information privacy, and of the extent of data harvesting practices on a corporate level. According to a related poll, 72% of the sample population had concerns about the possibility of corporations tracking their online activity (H. J. Smith et al., 2011). However, at the same time, online participants appear to have a positive response to relevant online corporate offers, in spite of being aware of the possibility of personal information tracking taking place by the same corporations. Approximately 82% of online users had a positive response to offers and discounts by online companies (Son & Kim, 2008). This is an interesting observation, as it underlines a conscious risk-taking approach regarding personal information privacy: the public expresses concern about companies mishandling their personal data, while accepting their promotions and offers. It is possible that such a behavior may be a temporary misjudgment of the severity of the possible privacy threat in light of a direct and tangible benefit, rather than a conscious and well-thought assessment of the situation in a broader context.

In the United Arab Emirates (U.A.E.), there are numerous laws that protect the information privacy of the public. These include, but are not limited to, the Computer Crime Act, the Data Protection Act, the Penal Code, and the Federal Constitution (Sarabdeen, Rodrigues, & Balasubramanian, 2014). However, despite the fact that such privacy laws are in place, a significant percentage of the public feel that their privacy is not secure. A related survey conducted in Dubai indicated that the public is concerned about both privacy in general, and information privacy in particular (Sarabdeen et al., 2014). 32.9% of Emiratis believe that the government should do more to protect their privacy (Pollock, 2018, December 17). At the same time, 66% of the public stated that they have reduced their exposure to social media, due to concerns over publicly expressing their views and the ability of third parties to access and use their data (Nair, 2016, May 4).

Based on the general concepts and ideas presented above, this study briefly discusses concepts related to information privacy and the emerging information technologies of Big Data (analytics), Cloud Computing and Services, and Internet of Things, and comments on the current status of information privacy within the U.A.E. in general.

INFORMATION PRIVACY AND BIG DATA

Data Scientists broadly categorize Big Data in terms of the 4 Vs of Information Technology: *Volume, Variety, Veracity,* and *Velocity* (Jagadish, 2015). Figure 1 illustrates the concept of Big Data using these four categories, and outlines its connections and structure in the context of the contemporary business environment. This structure defines and maps these categories according to their descriptor, function and size or quality:

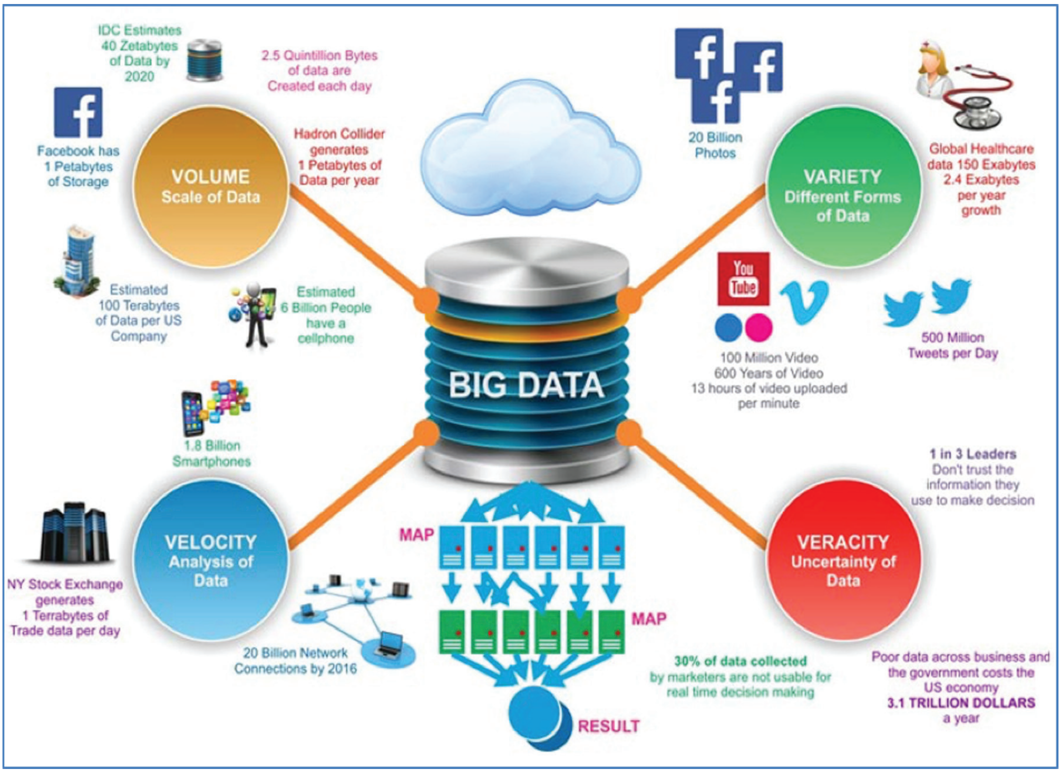
- *Volume of data* is substantial and can reach levels that are difficult for the average person to comprehend.
- *Variety of data* is large, ranging from traditional data types (e.g. audio, video, text) to contemporary ones (e.g. tweets and tags), while the data can be also categorized into structured or unstructured.
- *Veracity* is a descriptor based on the variety of data sources like smartphones, tablets, laptops, sensors, various types of wearables or online forms, and it suggests a high level of uncertainty.
- *Velocity* describes the volume of data per unit of time, and it can also reach substantial and difficult to contextualize levels.

The sheer volume and multifaceted nature of Big Data, makes it difficult not only to store, manage, and organize, but, more importantly, to subsequently process and analyze (Sagiroglu & Sinanc, 2013). The field of Big Data analytics is addressing such matters, with the aim to learning from the patterns, trends, and correlations that are extracted from it (Sagiroglu & Sinanc, 2013).

Admittedly, the above concepts are not new and have been examined in the context of various other fields of study (M. Smith, Szongott, Henne, & Von Voigt, 2012). However, with the recent advent of the combination of sophisticated and easily accessible technologies and networks, such as Cloud Computing, Internet of Things, and Smart Cities/ Houses/ Health, the significance and implications of Big Data has spread rapidly to multiple areas and human activities. Examples of this include, but are not limited to, government infrastructure and security, customer analytics, social media, or training, teaching and learning (M. Smith et al., 2012).

The broad availability and popularity of new technologies, and the subsequent rapid increase of interest on Big Data research and analysis has also led to a number of issues. Access to Big Data can be frequently misused, as in various cases of aggressive online promotions and targeted advertisement. A striking example of this is the case of a major U.S.-based business that used data mining to identify a pregnant teenager and send relevant vouchers for the expected baby, causing expressed dissatisfaction and stress to the expectant father (Xu, Jiang, Wang, Yuan, & Ren, 2014). This is just an example of a broader practice. The massive growth of online social platform usage has made users more vulnerable, as they become easy targets for the various social networking sites. However, similarly to other cases mentioned earlier, Stephen (2016) argues that many social media users trust the information privacy statements offered by the social media platforms, and ignore the risks that may be associated with

Figure 1. Big Data in terms of the 4 Vs of IT: Volume, Variety, Veracity, and Velocity (Cognixia, 2016, Nov. 5; Jagadish, 2015)


IDC Estimates 40 Zetabytes of Data by 2020
2.5 Quintillion Bytes of data are Created each day
Facebook has 1 Petabytes of Storage
VOLUME Scale of Data
Hadron Collider generates 1 Petabytes of Data per year
Estimated 100 Terabytes of Data per US Company
Estimated 6 Billion People have a cellphone
20 Billion Photos
VARIETY Different Forms of Data
Global Healthcare data 150 Exabytes 2.4 Exabytes per year growth
You Tube
100 Million Video 600 Years of Video 13 hours of video uploaded per minute
500 Million Tweets per Day
BIG DATA
1.8 Billion Smartphones
1 in 3 Leaders Don't trust the information they use to make decision
MAP
VELOCITY Analysis of Data
VERACITY Uncertainty of Data
NY Stock Exchange generates 1 Terrabytes of Trade data per day
MAP
20 Billion Network Connections by 2016
30% of data collected by marketers are not usable for real time decision making
Poor data across business and the government costs the US economy 3.1 TRILLION DOLLARS a year
RESULT

providing their personal information online. Partially, this may be due to the users being unaware of the effectiveness of analyzing the wealth of information provided by Big Data sources in exploiting personal information. Consequently, information privacy can be violated easier today than ever before (Zurbriggen, Ben Hagai, & Leon, 2016). This issue is exacerbated by the fact that businesses are striving to store, access, process, and analyze online data, as the obtained results can be decisive for the development and success of their business models. For example, Orbitz Worldwide Inc. organizes hotel advertisements based on the type of computers and software platforms used to make bookings. Based on their analysis, Orbitz observed that Mac users were 30% more likely to spend on bookings than PC users. Using this information, it advertised more expensive hotels to Mac users and cheaper ones to Windows PC users (Bujlow, Carela-Español, Sole-Pareta, & Barlet-Ros, 2017).

In order to avoid or limit the violation of information privacy, and have the data collectors protect their subjects' information privacy, the following suggestions can be brought forward:

- Access to collected data can be restricted only to authenticated and authorized users.
- Sensitive parts of the information can be hidden, in order for access to third parties to be controlled (Wu, Zhu, Wu, & Ding, 2013).

In the U.A.E., businesses, individuals, and the government share a similar experience of technology integration with other developed countries and regions around the world. The volume of online data storage is growing rapidly, thus creating a need for new ways of storing and protecting online information. Numerous initiatives exist within the public and the private sectors for the establishment of Big Data centers and related analytics processes. One public organization that is evidently actively involved in this is the U.A.E. Ministry of Energy. The latter engages in several Big Data initiatives, like the collaboration of all petrol station companies in the country in order to establish smart stations connected to a network through a newly developed mobile app. The app allows users to locate the nearest petrol station on a GPS-based system, and explore the services offered by the station. The information is updated by the petrol stations, and relevant transactions are stored on the Data Center (Sadaqat, 2015, June 10).

In terms of the impact of recent technological advances on a regional context, a significant shift of the local society towards using the internet more heavily is evident. As an example, according to information published on Hootsuite (2019), from a total population of 9.61 million, there are 9.52 million internet users (penetration level 99%), 9.52 millions active social media users (99%), and 8.80 millions mobile social media users (92%). Additionally, the average daily time spent using the internet via any device in the U.A.E. is 7 hours and 54 minutes, while the average daily time spent using any of the social media platforms via any device is 2 hours and 59 minutes. This is higher than the average daily viewing time for more traditional platforms, like broadcast and streaming, which was found to be around 2 hours and 30 minutes. This may be an indication that social media may have become the main connection and communication hub in the country. This, in turn, could suggest that the local users have started establishing a sense of belonging to the online communities and a redefined way of life heavily connected with online services, in line with similar observations and trends in other developed countries (Petronio, 2015).

The above is also reflected in what seems to be happening in the country from a consumer-based perspective, in the form of an increased use of online services. Hootsuite (2019) published that, in addition to the general public online and social media usage presented above, 83% of the internet users, which represents that vast majority of the population of the country, have conducted an online search for a product or service purchase. In addition, 92% have visited an online retail store, with 68% also purchasing something online using various different mobile devices.

The evident increased usage of online technologies within the country has not gone unnoticed by the local business sector in the U.A.E. Many companies are currently attempting to look deeper into Big Data, while a rather substantial number of companies in the U.A.E. are offering Big Data management and analytics services to their business partners (D'Mello, 2018, July 15). There are examples of such companies from various sectors, including oil and gas, medical, airlines, retail, finance, insurance, media, telecom, and hospitality, operating both within the public and private domains. On a broader scope, it is interesting to note that, currently, the U.A.E. is fifth in Big Data usage and analytics at an international level (D'Mello, 2018, July 15). This expressed interest, and the significant investments being made towards Big Data analytic services, showcase an underlying belief in the value of such services and their rewards. The strategic goal of this is rather clear: to understand customer requirements and try to meet them as closely as possible (D'Mello, 2018, July 15).

The initiatives and interest discussed above imply that vast amounts of personal data are stored online. As mentioned, this is something that can potentially threaten confidentiality and raise information privacy concerns. The significance of this matter is reflected on its apparent high priority for the U.A.E. government, expressed through its intent to protect the "freedom of communication by post, telegraph or other means of communication and the secrecy thereof" (Federal Law No. 5 of 2012 relating to Combating Information Technology Crimes, commonly known as Cyber Crimes Law), and the statement that "disclosing information obtained by electronic means is illegal where such information has been acquired illegally" (Federal Law No. 12 of 2016, Article 21) (UAE Government, 2019, Oct 23). Based on this, a violation of privacy in the U.A.E. can lead to civil action for damages pursuant to the Federal Law No. 5 of 1985 (the "Civil Code"), which specifies that anyone suffering *an unconstitutional infringement of their rights shall have the right to cease and seek compensation for the infringement.* In conjunction with the *right to privacy*, the Federal Law No. 3 of 1987 (the *Penal Code)* grants protection against the collection and release of personal data by individuals. The

Penal Code forbids the disclosure of private affairs, and imposes penalties of imprisonment and/or fines to anyone who publishes related news or pictures (Woods, 2018, May 22).

The above matters become relevant in the current scope, as one of the implications of the rapid increase of the use of the internet, online media, mobile devices, and online shopping platforms in the U.A.E. is the inevitable increase of information privacy risks for the general public. As local users of social media have already become targets of companies aiming at exploiting their online behavior and their, rather unwarranted, trust on social networking sites, provides an indication that these risks pose a real threat to the local society.

In an attempt to highlight and explore issues rising from the above observations, it is proposed that two different types of studies can be conducted in the broader area of Big Data analytics and the advent of social media:

- A study of the behavior and trust of the public towards online media. Such a study can provide useful qualitative and quantitative information and an insight on the potential privacy threats to the local society.
- An organized study of the level of deployment of Big Data infrastructure and provisions in the local business sector. This can include an assessment of the level of satisfaction from such investments from the perspective of executives or related companies, and their expectations for the near and long-term future.

The main aim of these studies will be to start a structured exploration of the changes the increased use of modern technologies, and the corresponding increase in the use and availability of Big Data, introduces to the local environment, in terms of information privacy of the individual. As part of this, the role and impact of local businesses as users of Big Data for commercial and advertisement purposes, as well as the role of the local government as a regulator of the availability and fair use of such data, should be studied and analyzed.

INFORMATION PRIVACY AND CLOUD COMPUTING

On a broader context, the term *Cloud Computing* refers to the on-demand availability of information systems hardware, software, networking, storage, and services, hosted on a third party's system instead of a local server or personal computer (Connell, 2012, February). A strict definition of the term may be difficult to come by, as it can describe a broad range of situations and applications within the broader context of IT. This becomes even more challenging, considering the growth rate of emerging technologies and the rapid transformation of the IT landscape in general (Vaquero, Rodero-Merino, Caceres, & Lindner, 2008). For the purposes of this study, it is sufficient to adopt the broader definition given by the National Institute of Standards and Technology (NIST) that Cloud Computing describes a "model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort" (D. Chen & Zhao, 2012).

In terms of contextualizing the term into more specific and detailed components, Mell and Grance (2011) also describe Cloud Computing services that can be categorized based on their function and usage from the perspective of the consumer:

- *Cloud Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.*
- *Cloud Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider.*

- *Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.*

This model is illustrated in Figure 2.

Irrespectively of the exact structure and definition used, what can be claimed about Cloud Computing systems is that they have become increasingly common and relevant. This is unsurprising, as the cost of establishing and maintaining a sophisticated IT infrastructure that can keep up with the rapid technological developments and the constant change of tools and hardware has increased dramatically, even though information technology equipment costs are generally decreasing. As companies seek ways to reduce running costs, more efficient and flexible ways of working with complex IT systems are required. In this context, Cloud Computing assists by transferring the costs related to IT infrastructure and maintenance to third party providers (Vaquero et al., 2008). As an example of this, Figure 3 depicts the dramatic rise of revenue from Cloud services worldwide in billions of U.S. dollars (Shanhong, 2019, Oct. 30).

Similar observations can be made in the U.A.E. and the MENA regions (Middle East and North Africa). Local businesses and government organizations are trying to follow global developments and adapt to the rapidly changing environment created by the emerging technologies (Khehar, 2018, October 4), with Cloud Computing services offering the potential for development of the infrastructure to become:

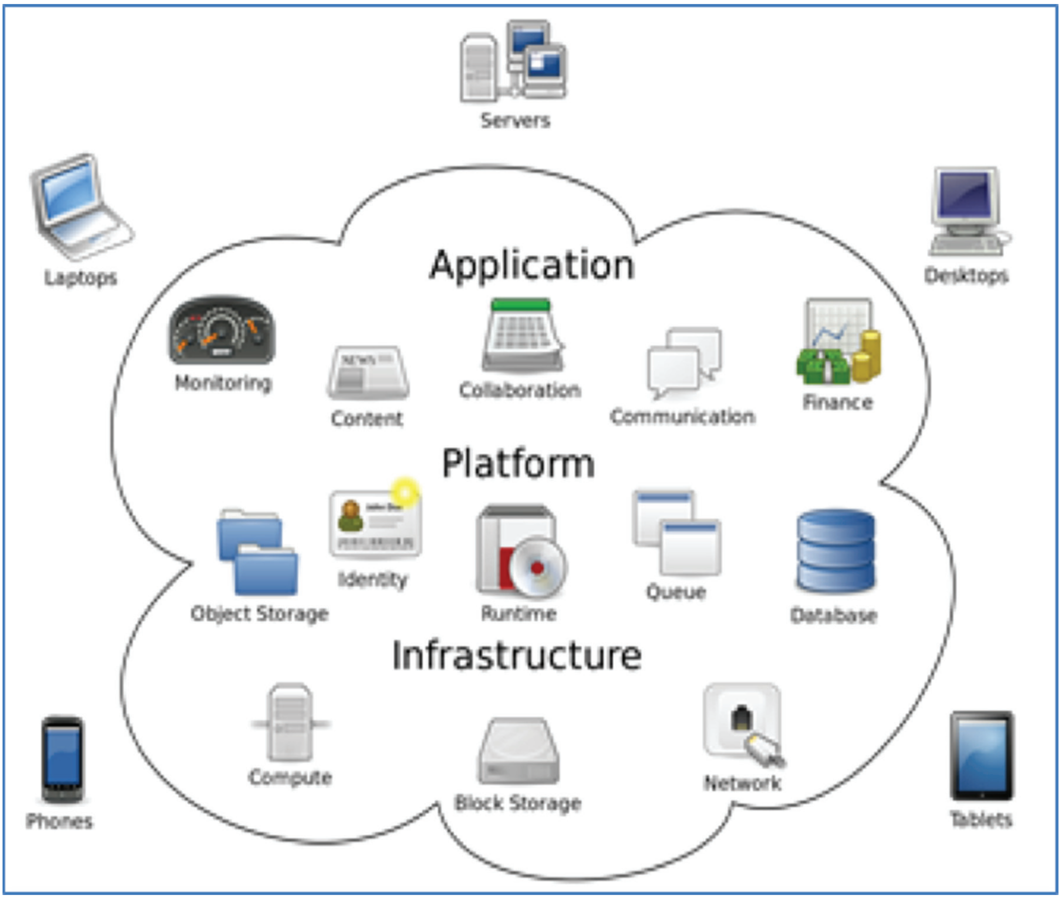
- rapid,
- effective,
- available on-demand, and
- scalable.

Increased business activity on a global level could dictate that countries may need to accelerate both their digital transformation and economic diversification (Bridge, 2019, March 1; W. Chen, 2011). Thus, the regional state regarding the use of Cloud services should grow to a point that is comparable with those in other developed countries. This is also reflected in the projections for Cloud services revenue, indicating that it is likely to quadruple from its 2015 level by 2020 (Figure 3).

In terms of the implementation and challenges of adopting such services more extensively, Cloud Computing systems can be implemented at reasonable costs that can be significantly lower than those of similar systems built in-house and utilizing local private resources. The apparent benefits of using such systems are reflected on the current state of the business sector in the U.A.E. According to a report undertaken by Dubai Silicon Oasis Authority and IBM, at the present time there is a 70% penetration of Cloud-based services in the case of start-up companies (Gulf News Tech, 2017, December 18), while in terms of the value and future of such services on a local basis in general, it is suggested that approximately 32,000 new jobs could be created in the country as a direct result of this transition (Sharma, 2019, Jan. 1). As an example, Microsoft has already announced Cloud data centers in Abu Dhabi and Dubai, while Dubai Airports currently use Microsoft's Azure Cloud service for the Wi-Fi services offered to travelers. This observation becomes even more interesting considering that Azure has a 16% share of the global Cloud infrastructure market, making Microsoft the second-biggest provider of cloud services after Amazon's Web Services.

Despite its many benefits, Cloud Computing poses its own information privacy threats and challenges. One of the main problems with Cloud Computing in relation to information privacy, is that it involves the process of transferring big volumes of data between servers across the world. This means that the process exceeds national boundaries and, thus, introduces potential security and privacy risks that the public may not be aware of (Wang, Zhao, Jiang, & Le, 2010).

Figure 2. Illustration of a cloud computing model according to Ward and Peppard (2002)

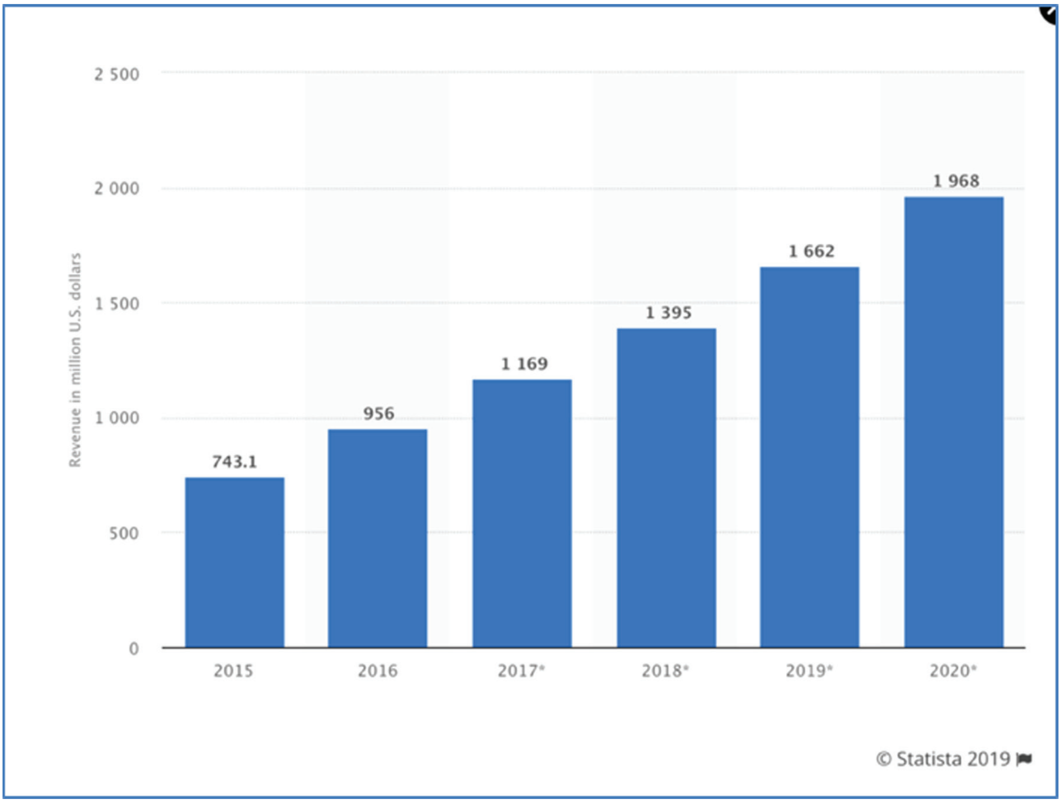


This is especially true in cases where one side of the process resides in a country with loose legal systems in terms of protection from malpractices related to digital systems. This has led specific countries to take specific measures to address such issues. For example, one could consider the case of the U.S. passing a law that required Cloud providers to disclose emails stored in their servers. Similarly, in the E.U., the General Data Protection Regulation (GDPR - implemented in May 2018), regulates the transfer of personal data, both within and outside the E.U. boundaries, with the aim of protecting the information privacy of the public. Such measures attempt to address data security by controlling the storage methods of data in the Cloud, ensuring transparency of the Data Location, and enforcing Data oversight (i.e. making sure Cloud providers follow appropriate and updated policies and regulations) (Kirkpatrick, 2018). Irrespectively of whether one adopts the perspective of the government or the individual, there are certain concerns that need to be addressed:

- Who has control over personal data?
- Who has control over the disclosure of the data?
- How transparent is the regulatory and functional framework?

Similarly, to other developed and developing countries, in the U.A.E., there is currently a high interest in Cloud Computing technologies. This raises concerns in relation to the legal framework

Figure 3. Revenues from cloud services in the MENA region between 2015 and 2020 (Oommen, 2019, June 24)



that may be needed in order to regulate and safeguard local businesses against potential threats. At present, there are no particular laws to govern this newly formed ecosystem in the U.A.E. (Yates, 2011). The local business sector is only supported by general laws that may, or may not, apply to the unique cases that may be encountered while transitioning to a Cloud-based model. As such, one has to rely on the effect of the various U.A.E. laws governing the security of private data, data collection, and their application to cases related to Cloud providers. It is useful to note that Cloud providers in the country are required by law to put adequate protection measures in place, in order to prevent failures that might lead to loss of data, security breaches, or other violations of information privacy. It must be noted that it is possible to have multiple businesses or entities collaborating to provide such services, while their clients are often unaware of the fact that different companies are involved in this process (Yates, 2011, June).

Two distinct ways of temporarily addressing this gap of legislation in the country are proposed. The first is by conforming to the ISO 27001 manual, which outlines the criteria for creating, implementing, running, tracking, evaluating, maintaining, and enhancing an ISM Certification (ISM Institute for Supply Management, 2019). This particular certification demonstrates that the Cloud service provider has introduced a broad range of security and privacy controls at certain levels of the business, and that all employees are adequately trained in terms of the security and privacy policies and practices that are in place. The second is by enforcing the U.A.E. Commercial Transaction Law (Federal Law No. 18 of 1993), which sets the general requirements for the retention of advertisement documents for a period of at least five years from the date of issue or receipt (Connell, 2014, January).

In addition to the above, one of the main concerns arising from the use of services based on Cloud Computing systems has to do with potential security vulnerabilities of these services that could compromise information privacy and the confidentiality of the customers' data. The reason behind the increased threat posed by this, is that a single security breach in one of the services might expose various others parts of the service to additional threats (D. Chen & Zhao, 2012). Furthermore, since the Cloud service providers managing the system have full access control, concerns about the ways the data could be used are also increased (Ryan, 2011).

Considering issues such the ones presented above, it is suggested that investigating concepts and ideas related to both Cloud Computing structure and its impact on information privacy becomes an interesting and timely quest. It is proposed that further work in this direction may include, but is not limited to, the following:

- A structured study of the penetration of Cloud Computing services in the country and the users' preferences in relation to it.
- A structured study of the executives' perspective regarding the financial benefits and implications of adopting such a paradigm.
- An investigation of whether the local workforce is prepared to follow this new trend in terms of skills, training, and experience.

One of the aims of such studies should be to start a structured exploration of the current state of Cloud Computing usage and infrastructure in the country, and attempt to assess and evaluate the potential impact of future developments in this area. Ultimately, this could be used as a springboard for the informed assessment of potential information privacy issues and challenges arising from the extensive use of such services, and for the proposal of potential solutions for any identified issues.

INFORMATION PRIVACY AND INTERNET OF THINGS

As the digital world is growing at an ever-increasing pace, a vast number of digital devices are interconnected via the internet, a concept known as Internet of Things (IoT). This describes a network of devices facilitating one's access to different sources of data anywhere and anytime, hence the term being ubiquitous, regardless of the type of the device. An interesting observation in relation to Internet of Things is that there are more digital devices connected to the Internet than the total population worldwide. Figure 4 illustrates this fact and projects the underlying trend to a short-to-medium term horizon (Waterford Technologies, 2018).

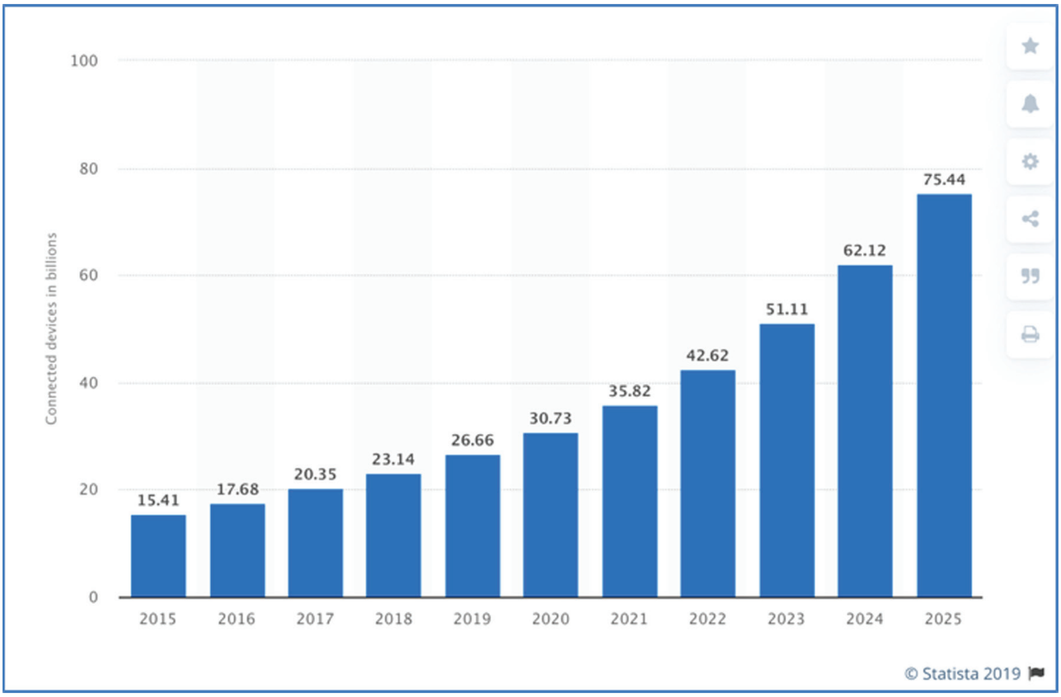
In a broader context, Internet of Things is a term used to describe an interconnected ecosystem of:

- devices,
- possible communication between these devices and users, and
- the exchange of data of various forms between them (Postscapes, 2019, March 21).

At the present time, IoT is extensively used for the automation of processes that, until recently, were completed manually (Tan & Wang, 2010). One example of this is Amazon Alexa, a virtual assistant that facilitates the automation of, otherwise manual, processes through Artificial Intelligence (AI) (Kushma, 2018, September 2). Another relevant example is that of Radio Frequency Identification (RFID) technology that is one of the cornerstones of IoT applications used in numerous human activities, such as in automatic electronic tolls (Tan & Wang, 2010).

Admittedly, applications such as the ones described above, provide various benefits. However, privacy concerns could also be raised as IoT utilization grows, similarly to these relating to other technological developments that rely heavily on the use of the internet. A good example of this is a reported case of privacy invasion in the U.S.A., when a *smart speaker* recorded one of the private conversations of a couple and shared it with random contacts (Fowler, 2018, May 24). Information

Figure 4. Internet of Things. Connected devices in billions (Waterford Technologies, 2018, March 15).



privacy issues such as these become even more alarming considering the unprecedented levels of interconnectivity over the internet. Such issues, tied with the sheer volume of information stored and shared online intensify privacy concerns. In terms of dealing with such issues, it has been suggested that a holistic approach is required, as this will address problems of security and privacy at multiple possible levels concerning *"platform security, secure engineering, security management, identity management, industrial rights management"* (Sadeghi, Wachsmann, & Waidner, 2015). Such ideas have led to technology companies launching and utilizing software specifically aiming at addressing information privacy concerns. A good example of this is *PrivacyCheck*, a browser extension released by Google. This facility resides in the start button and, once triggered, it extracts a text of privacy policy, reprocesses it, and transfers it to a data mining model, set to determine the risk level based on ten privacy factors. It then displays the risk level as follows:

- green = low risk,
- yellow = medium risk
- red = high risk.

The software then attempts to highlight the risk and describe it in detail when the user hovers upon certain items (Zaeem et al., 2018).

Dubai is considered a Smart City. The local community is working towards a full adoption of emerging technologies and advanced digital infrastructures. Such moves are projected to lead to significant transformations. For instance, savings of up to 40% are expected in terms of electricity costs (Cherrayil, 2018, October 17), while socially transformative developments like a proposed IoT system by the Civil Defense that detects and warns the local residents in cases of fire using AI features are also in motion. Such developments can have a significant impact on the local environment. Recognizing the dynamics within the country, and in light of the decision to move towards the Smart

City paradigm, the Dubai Government has launched a new program that aims at protecting information security and privacy in the Emirates. The new initiative, called Dubai Digital Certificates, is a joint effort between the Smart Dubai Office and the Dubai Electronic Security Center (DESC). Under the program, entities involved *"will be authorized to issue reliable digital certificates, allowing them to exchange information securely through their digital services, as well as other applications"* (Sutton, 2017, Oct. 23; The National, 2017, Oct. 22). This MoU is the government's response to the various concerns about the rapid information technology developments encompassing and incorporating Big Data, Cloud Computing, Internet of Things (IoT), Blockchain, and Artificial Intelligence.

As local applications of IoT can be varied and rather specialized, an in-depth discussion of this matter exceeds the scope of this study. However, in a broader context, Dubai's strategy on Internet of Things generally aims to:

- protect digital wealth,
- encourage government departments to join the emirate's smart transformation,
- achieve the objectives of the Smart Dubai Plan 2021.
- facilitate the transition to the outlined goal of a 100% paperless government. This particular strategy covers six strategic domains [29]:
    - governance,
    - management,
    - acceleration,
    - deployment,
    - monetization, and
    - security.

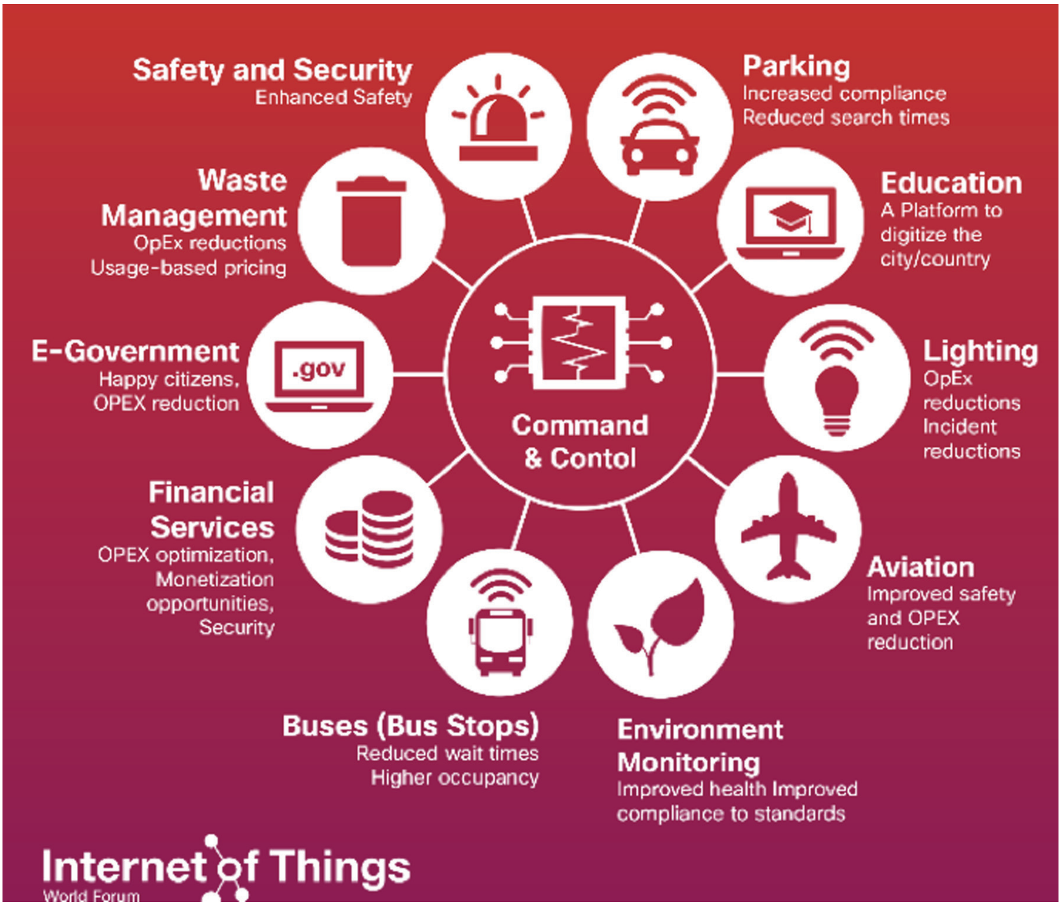
Ultimately, utilizing best practices in order to facilitate the Smart City Dubai strategy (Figure 5) is expected to benefit the U.A.E. to achieve the goals set by the vision of His Highness Sheikh Mohammed bin Rashid Al Maktoum. In this context, it is both interesting and relevant to study the scope and level of the IoT penetration in the country, and to analyze the qualitative elements of this penetration and its prospects in the years to come. This is especially interesting in terms of the perspective of the local population regarding the impact of such developments on information privacy. It is suggested that further studies in this direction could focus on specific aspects of the emerging uses of IoT that can have a direct impact on the local society and businesses.

CONCLUSION

The increased interest on, and use of, platforms and systems utilizing emerging technologies like Big Data (analytics), Cloud Computing services, and Internet of Things (IoT), bring along many benefits that can greatly affect corporate and personal activity, and reshape global societies, the business landscape, and human life in general. However, this comes at a cost. Among the most important aspects of human life that may be affected by such developments is that of personal information privacy. It probably goes without saying that no benefit outweighs this basic human right. There is a need to find a balance between the multiple benefits of the technological developments, and the protection of basic human rights like personal information privacy.

U.A.E. is moving towards adopting modern emerging technologies, while also establishing a framework of policies and laws to protect the local public from possible abuse. Although significant progress has been made, more work is still required in this direction. Future research should take into account both the potential issues and challenges, and any concerns raised in relation to the prospect of fully adopting such technologies.

Figure 5. Dubai IoT and Smart city best practices. (UAE Government, 2019, Oct. 1)



This paper aims at providing a preliminary overview of the relevant developments in the country, and their effect on the information privacy of the local population. Research questions and themes pointing to possible directions for further study have been briefly suggested and outlined. Such questions and themes include, but are not limited to, the following:

- What is the level of deployment of Big Data infrastructure in the local business environment? What is the level of satisfaction from these investments from the viewpoint of the executives of these companies and what are their expectations for the near future?
- What is the penetration level and the appropriate type of Cloud Computing services in the country? How do the local executives perceive the financial benefits of following such paradigms, and how prepared is the local workforce to follow this trend in terms of skills and appropriate experience?
- What is the penetration level and scope of the application of IoT in the country? What is its effect on the public's perception of Information Privacy?
- How is it expected that the above developments will affect one of the most important human rights, i.e., that of information privacy, in the context of U.A.E.

REFERENCES

Bridge, S. (2019, March 1). *Microsoft ecosystem to create 5,600 Bahrain jobs by end-2022*. Retrieved from https://magnitt.com/news/41225/microsoft-ecosystem-create-5600-bahrain-jobs-end-2022

Bujlow, T., Carela-Español, V., Sole-Pareta, J., & Barlet-Ros, P. (2017). A survey on web tracking: Mechanisms, implications, and defenses. *Proceedings of the IEEE*, *105*(8), 1476–1510. doi:10.1109/JPROC.2016.2637878

Chen, D., & Zhao, H. (2012). *Data security and privacy protection issues in cloud computing*. Paper presented at the 2012 International Conference on Computer Science and Electronics Engineering. doi:10.1109/ICCSEE.2012.193

Chen, W. (2011). *Cloud Computing in the UAE Context: An institutional perspective*. Paper presented at the International Conference on Information Resource Management (Conf-IRM).

Cherrayil, N. K. (2018, October 17). *UAE to be ready for mass IoT adoption by 2020*. Retrieved from https://gulfnews.com/technology/uae-to-be-ready-for-mass-iot-adoption-by-2020-1.2290880

Cognixia. (2016, Nov. 5). *Bigger Opportunity – Become an Expert in Big Data*. Retrieved from https://www.cognixia.com/blog/bigger-opportunity-become-expert-big-data

Connell, N. O. (2012, February). *Data Protection and Privacy Issues in the Middle East*. Retrieved from https://www.tamimi.com/law-update-articles/data-protection-and-privacy-issues-in-the-middle-east/

Connell, N. O. (2014, January). *Legal Issues in Cloud Computing – Part I*. Retrieved from https://www.tamimi.com/law-update-articles/legal-issues-in-cloud-computing-part-i/

D'Mello, S. (2018, July 15). *Big data for bigger opportunities*. Retrieved from https://www.khaleejtimes.com/technology/big-data-for-bigger-opportunities

Fowler, G. A. (2018, May 24). *Hey Alexa, come clean about how much you're really recording us*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/hey-alexa-come-clean-about-how-much-youre-really-recording-us/?noredirect=on&utm_term=.3c96d4fc293d

Gulf News Tech. (2017, December 18). *70% of Dubai start-ups employ cloud computing. 24% even built their start-ups on the cloud, Cloud Report 2017 reveals*. Retrieved from https://gulfnews.com/technology/70-of-dubai-start-ups-employ-cloud-computing-1.2143319

Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *Management Information Systems Quarterly*, *37*(1), 275–298. doi:10.25300/MISQ/2013/37.1.12

Hootsuite. (2019). *The global state of digital in 2019*. Retrieved from https://hootsuite.com/en-gb/resources/digital-in-2019

Ipsos. (2019, Jan. 25). *Ignorance and Distrust Prevail about What Companies and Governments Do with Personal Data*. Retrieved from https://www.ipsos.com/en/ignorance-and-distrust-prevail-about-what-companies-and-governments-do-personal-data

ISM Institute for Supply Management. (2019). *Make the Investment in You*. Retrieved from https://www.instituteforsupplymanagement.org/certification/content.cfm?ItemNumber=30150&SSO=1

Jagadish, H. V. (2015). Big data and science: Myths and reality. *Big Data Research*, *2*(2), 49–52. doi:10.1016/j.bdr.2015.01.005

Khehar, A. (2018, October 4). *How the cloud is helping the UAE's digital transformation*. Retrieved from https://www.khaleejtimes.com/technology/how-the-cloud-is-helping-the-uaes-digital-transformation

Kirkpatrick, K. (2018). Borders in the Cloud. *Communications of the ACM*, *61*(9), 19–21. doi:10.1145/3237072

Kushma, K. (2018, September 2). *Integrating Amazon Alexa into IoT Ecosystem*. Retrieved from https://iotdunia.com/integrating-amazon-alexa-iot-ecosystem/

Mell, P., & Grance, T. (2011 Sep). *The NIST Definition of Cloud Computing*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-145/final

Nair, M. (2016, May 4). *Middle East social media users spooked by privacy*. Retrieved from https://gulfnews.com/technology/media/middle-east-social-media-users-spooked-by-privacy-1.1819032

National Commissions for UNESCO. (2010, Jan. 4). Claiming Human Rights. *The Universal Declaration of Human Rights.* Retrieved from http://www.claiminghumanrights.org/udhr_article_12.html - at13

Oommen, A. (2019, June 24). *Time for UAE businesses to get their head in the "clouds"*. Retrieved from https://www.ameinfo.com/industry/technology/uae-business-cloud-service-data-center

Petronio, S. (2015). Communication privacy management theory. The International Encyclopedia of Interpersonal Communication, 1-9.

Pollock, D. (2018, December 17). *UAE Public Privately Split on Key Issues, New Poll Reveals*. Retrieved from https://www.washingtoninstitute.org/fikraforum/view/in-private-uae-public-split-on-key-issues-new-poll-reveals

Postscapes. (2019, March 21). *IoT Devices & Products*. Retrieved from https://www.postscapes.com/internet-of-things-award/winners/

Ryan, M. D. (2011). Cloud computing privacy concerns on our doorstep. *Communications of the ACM*, *54*(1), 36–38. doi:10.1145/1866739.1866751

Sadaqat, R. (2015, June 10). *UAE ready for big data technology, experts say*. Retrieved from https://www.khaleejtimes.com/business/local/uae-ready-for-big-data-technology-experts-say

Sadeghi, A.-R., Wachsmann, C., & Waidner, M. (2015). *Security and privacy challenges in industrial internet of things.* Paper presented at the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC). doi:10.1145/2744769.2747942

Sagiroglu, S., & Sinanc, D. (2013). *Big data: A review.* Paper presented at the 2013 International Conference on Collaboration Technologies and Systems (CTS). doi:10.1109/CTS.2013.6567202

Sarabdeen, J., Rodrigues, G., & Balasubramanian, S. (2014). E-Government users' privacy and security concerns and availability of laws in Dubai. *International Review of Law Computers & Technology*, *28*(3), 261–276. doi:10.1080/13600869.2014.904450

Shanhong, L. (2019, Oct. 30). *Cloud infrastructure services market revenue worldwide from 1st quarter 2016 to 3rd quarter 2019*. Retrieved from www.statista.com/statistics/967292/worldwide-cloud-infrastructure-services-market-revenue

Sharma, A. (2019, Jan. 1). *How the cloud will create nearly 32,000 jobs in the UAE*. Retrieved from https://www.thenational.ae/business/technology/how-the-cloud-will-create-nearly-32-000-jobs-in-the-uae-1.808495

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *Management Information Systems Quarterly*, *35*(4), 989–1016. doi:10.2307/41409970

Smith, M., Szongott, C., Henne, B., & Von Voigt, G. (2012). *Big data privacy issues in public social media.* Paper presented at the 2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST). doi:10.1109/DEST.2012.6227909

Son, J.-Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *Management Information Systems Quarterly*, *32*(3), 503–529. doi:10.2307/25148854

Stephen, A. T. (2016). The role of digital and social media marketing in consumer behavior. *Current Opinion in Psychology*, *10*, 17–21. doi:10.1016/j.copsyc.2015.10.016

Such, J. M., & Criado, N. (2018). Multiparty privacy in social media. *Communications of the ACM*, *61*(8), 74–81. doi:10.1145/3208039

Sutton, M. (2017, Oct. 23). *Dubai Digital Certificates to secure government processes, Initiative from Smart Dubai Office and DESC to create certification scheme for government*. Retrieved from https://www.itp.net/615446-dubai-digital-certificates-to-secure-government-processes

Tan, L., & Wang, N. (2010). *Future internet: The internet of things.* Paper presented at the 2010 3rd international conference on advanced computer theory and engineering (ICACTE).

The National. (2017, Oct. 22). *Sheikh Mohammed launches Internet of Things Strategy in Dubai*. Retrieved from https://www.thenational.ae/uae/government/sheikh-mohammed-launches-internet-of-things-strategy-in-dubai-1.669413

UAE Government. (2019a, Oct 23). *Data and privacy protection in the UAE*. Retrieved from https://www.government.ae/en/about-the-uae/digital-uae/data/data-and-privacy-protection-in-the-uae

UAE Government. (2019b, Oct. 1). *Dubai Internet of Things Strategy*. Retrieved from https://www.government.ae/en/about-the-uae/strategies-initiatives-and-awards/local-governments-strategies-and-plans/dubai-internet-of-things-strategy

Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2008). A break in the clouds: Towards a cloud definition. *Computer Communication Review*, *39*(1), 50–55. doi:10.1145/1496091.1496100

Wang, J., Zhao, Y., Jiang, S., & Le, J. (2010). *Providing privacy preserving in Cloud computing*. Paper presented at the 3rd International Conference on Human System Interaction. doi:10.1109/HSI.2010.5514526

Ward, J., & Peppard, J. (2002). The evolving role of information systems and technology in organizations: A strategic perspective. *Strategic Planning for Information Systems*, 1-59.

Waterford Technologies. (2018, March 15). *Just How Big is Big Data?* Retrieved from https://waterfordtechnologies.com/just-big-big-data/

Woods, V. (2018, May 22). *Privacy and Data Protection in the UAE*. Retrieved from http://www.hadefpartners.com/News/329/Privacy-and-data-protection-in-the-UAE-:~:targetText=The%20UAE%20Constitution%20addresses%20privacy,in%20accordance%20with%20the%20law%E2%80%9D

Wu, X., Zhu, X., Wu, G.-Q., & Ding, W. (2013). Data mining with big data. *IEEE Transactions on Knowledge and Data Engineering*, *26*(1), 97–107.

Xu, L., Jiang, C., Wang, J., Yuan, J., & Ren, Y. (2014). Information security in big data: Privacy and data mining. *IEEE Access : Practical Innovations, Open Solutions*, *2*, 1149–1176. doi:10.1109/ACCESS.2014.2362522

Yates, D. (2011, June). *Cloud computing in the UAE: Legal risks and remedies for providers and users.* Retrieved from https://www.tamimi.com/law-update-articles/cloud-computing-in-the-uae-legal-risks-and-remedies-for-providers-and-users/

Zaeem, R. N., German, R. L., & Barber, K. S. (2018). PrivacyCheck: Automatic Summarization of Privacy Policies Using Data Mining. *ACM Transactions on Internet Technology*, *18*(4), 53. doi:10.1145/3127519

Zurbriggen, E. L., Ben Hagai, E., & Leon, G. (2016). Negotiating privacy and intimacy on social media: Review and recommendations. *Translational Issues in Psychological Science*, *2*(3), 248–260. doi:10.1037/tps0000078

Dimitrios Xanthidis holds a PhD in Information Systems from the University College London. The past 25 years he is teaching in tertiary education various Computer Programming, Databases, and relevant courses and is conducting research on themes related to Social Media, eCommerce, eHealth, and eLearning. Currently he is with Higher Colleges of Technology in Dubai, U.A.E.

Christos Manolas is an audio, media and technology specialist with academic and professional experience in music performance and technology, media production, sound design, multimedia and IT. Chris' diverse background makes him an all rounder with skills in several areas, including but not limited to, sound synthesis and audio signal processing, audiovisual media production, audio engineering, music performance and composition, and software development.

Ourania Koutzampasopoulou Xanthidou holds a M.Sc. in Computer Science from the University of Malaya, Kuala Lumpur, Malaysia. She has more than 15 years of involvement with the IT industry as support of IT departments of SMEs and about 5 years of teaching experience in tertiary education. Her research interests are in the areas of eHealth, Smart Health, databases, web programming and object-oriented programming.

Han-I Wang is a research fellow in the Mental Health and Addiction Research Group (MHARG). She completed her Doctorate in health economics at the University of York in 2011 and worked in the Epidemiology & Cancer Statistics Group (ECSG) (2011-2019) before joining MHARG in 2019. Han-I specialises in cost analysis, health outcome research and decision modelling using complex patient level data. Her main research interests are in the exploration of different decision modelling techniques and their application to predict healthcare expenditure, patients' quality of life and life expectancy. Han-I has research experience on various disease areas and works closely with academic research teams and government bodies both inside and outside the University.