Kids and Parents Privacy Exposure in the Internet of Things: How to Protect Personal Information?

Maria G. Vallejo, Gabriela E. Muñoz, Jonathan Hernando Rosales

Universidad Autónoma de Guadalajara, Guadalajara,
Mexico
lupita_vallejo_valencia@hotmail.com, {gabriela.munoz, jonathan.rosales}@edu.uag.mx

Abstract. The paradigm of communication "anywhere, any way and at any time" of mobile and universal computing extends to "anything, any person and any service" with the Internet of Things (IoT). There are more and more users adopting these technologies that generate significant amounts of information. However, there are individuals and institutions (public and private) that seek to triangulate some of this information with various purposes, not always with good intentions. Most people are unaware of the threats that exist on-line, and it is unlikely for them to seek protection from something they ignore. This paper seeks to bring awareness towards the risks that exist when providing personal information on-line, particularly by pointing out some advice for the protection of sensitive data regarding children and their families. A broad description of how Mexican parents deal with their children's activities on the internet is the starting point for a culture of awareness, education and protection of the children's information security and privacy on-line.

Keywords. Exposure, family, internet, IoT, risk, social networks.

1 Introduction

It seems that the next step of the current transformation in society is for the "Internet of Things" (IoT) to consolidate [2, 9]. Where the internet connects not only people but also machines, smart objects and things thanks to wireless and wired connectivity [16, 21]. The current paradigm of communication "anywhere, in any way and at any time" of mobile and ubiquitous computing extends the paradigm to "anything, any person and any service" with the IoT [22].

The "marketing of IoT is estimated to reach $ 309 billion per year by 2020" [16]. The "potential economic impact of IoT will reach $ 2.7 trillion to $6.2 trillion per year by 2025" [21]. "Although the estimations of marketing value for IoT and its relevant applications from different research fields are different", they concur in the fact that it will strongly impact the industries and economies soon. By using technologies of IoT in daily life, fast and convenient interactive environments can be expected [21]. Tools, devices and processes can be easily controlled, monitored, and coordinated.

For example, the status (i.e., activity or location) of shipments can be tracked on-line in real time. Thus, things can be monitored and managed more effectively and efficiently, providing better services to users. The devices of the IoT may be located in fixed places or may be moved from one place to another. Several of these interconnected devices can provide up-to-date data related to the current state and identity of the person, location, behavior and/or environmental conditions. The management of this data dissemination is left to the owner of the object or to a trusted operator.

Therefore, the protection of personal privacy becomes increasingly a history of protection of electronic data, becoming a mixture of advantages, challenges and risks. The frequent simplistic response of many Internet users "I am not worried about privacy and/or I do not have anything to hide" makes it even more complicated to protect the personal information of those who are not aware about existing online threats, especially children.

The accumulation of large volumes of information, combined with data mining and artificial

Computación y Sistemas, Vol. 22, No. 4, 2018, pp. 1191–1205
ISSN 1405-5546
doi: 10.13053/CyS-22-4-3082

intelligence, allows personal data to be analyzed and linked by third persons: individuals and companies that are interested in collecting private information, but not always with good intentions [6]. About privacy, Thomas P. Keenan signals out “The growing problem of Internet data persistence” stating that the problem of information getting into the wrong hands has existed since the first stored data computer system [10], but that it can now get there much faster due to the ease of access to it, and to how information travels all around the world raising the privacy problem to a public issue.

Considering each and every day more people become Internet users, owners of a smartphone or active within on-line social networks, it is reasonable to ponder “Where is the information we send stored?, Who has access to it?, What can be done with this information?, and, most importantly, How is its privacy protected?” and to bring attention towards how some internet users show ignorance or lack of concern regarding their private information generated, gathered, and potentially being exposed by the IoT.

The purpose of this paper is to promote awareness among internet users by discussing the risk of third parties having access to personal data -particularly that belonging to children- within the transformations brought about by the IoT. After establishing the meaning of some widely used key concepts, the relationship between awareness and ignorance of technical and non-technical privacy measures, and how it propitiates vulnerability to the risks and dangers of the IoT, will be explored and described based on broad statistical information gathered from mexican families and the criteria with which they manage their activity on-line regarding personal information.

2 The Fast-Growing of Internet Usage and Personal Privacy Affectation

The extent of its capabilities and its potential to radically change the way we live has brought the IoT to the spotlight around the world. Nowadays, internet access has become widely available as the cost of connectivity infrastructure decreases, more Wireless Fidelity (WIFI) capable devices are available for a variety of fields and purposes (from health to entertainment), and smartphone sales keep on the rise. These factors create “the perfect storm”, as Jacob Morgan from Forbes magazine states [17], allowing people to communicate with one another regardless of borders and providing an ever increasing number of services that can be accessed anywhere by anyone.

It is important to approach these complex -and often hermetic- technologies through non-exclusive definitions of key concepts - such as “the internet” and “privacy”, for example - that allow laymen to discuss, and hopefully understand, some of the processes involved which might concern the way personal information is gathered, managed and treated by third parties.

2.1 What is “The Internet”?

The Oxford Dictionary, defines “the Internet” as a global computer network that provides a variety of information and communication facilities, consisting of interconnected networks, using standardized communication protocols [19]. The Cambridge Dictionary adds that it provides information on very many subjects and enables users to exchange messages [5] allowing people and systems to communicate easier, faster regardless of their physical location. According to the AMIPCI [8] Mexico’s fast-growing internet users have gone from 20.2 million users to 53 million users from 2006 to 2014 [1]. Public of private WIFI is the preferred connection method used, mainly, for social networks (85%), sending/receiving emails (73%), and music downloading.

Having statistics about the type of connection that users opt to use and the kind of transactions made helps identifying the ease with wich someone’s information might be stolen due to the likelihood of somebody sniffing on a public network (airports, coffee shops, etc.). The number of children using the Internet is significant (83% of 662) with a start age, according to 43% of the parents, of 3-6 years old merely for entertainment (58%) and because of school (40%).

As stated in Figure 1, smartphones and tablet computers are the devices that have increased internet access penetration. Contrastingly, desktop computers have lost presence as portability

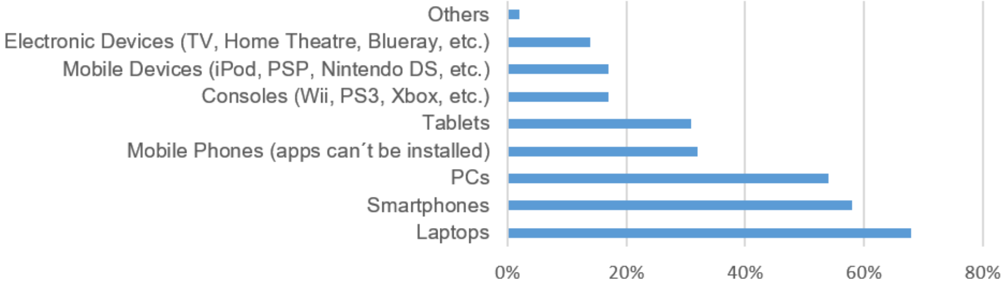

Fig. 1. Devices Connected to Internet in Mexico by [1]

becomes one of the main advantages of newer devices. Other devices, such as game consoles and smart TVs remain without significant growth [1].

2.2 What is Privacy?

Privacy is often confused with security [3], thus creating a false bifurcation which is not discussed in this paper. However, if we mention for the moment that security and privacy are at opposite ends, balance should be sought after.

The current limits of what privacy means today, are still fluid and unclear. Laborde et al. [6] have compiled some definitions that consider the newreaches provided by communication and computing technologies. Warren and Brandeis [25] described privacy as “the right to be let alone and to keep personal matters and relationships in secret”.

However, Langheinrich [12] states that privacy alludes to the freedom from damaging publicity, public scrutiny, secret surveillance, or unauthorized disclosure of one’s personal data or information by a government, corporation, or individual; pointing out that preserving privacy through isolation is no longer an option in today’s world. This definition is the most accurate because it encompasses the “right to be let alone” stating very clearly that it concerns not only individuals but also corporations or institutions.

By Gary Marx [14] privacy is usually perceived by users as an expectation of being in a state of protection without having to actively pursue it. Users feel concerned when their privacy gets violated. In the same vein, Marx mentions three important elements that are directly connected with violations of privacy. The first one is confidentiality which objective is to protect personal context data from being accessed by unauthorized persons (something that can only be found in a few existing privacy technologies). Then there is privacy as control, that refers to the ability to manage what happens with personal data and to avoid its undesired use.

This encompasses technologies for specifying and enforcing privacy policies. Hence, if personal data becomes public, confidentiality and thus privacy are lost. Privacy, as much as confidentiality, represent the solution for anonymizing the collected data. Lastly, Marx [14] states that “anonymity of data relies on cryptographic solutions to achieve certain properties like ’unlinkability’ (two information items or actions of the same user cannot be related), ’undetectability’ (an attacker cannot distinguish whether an information item exists), ’unobservability’ (it is not possible to detect whether a system is being visited by a given user) and communications content confidentiality”.

Governments all over the world started to be concerned about this and began creating laws and regulations for privacy to help citizens to feel protected against this phenomenon. It is no different in Mexico where the Federal Law of Personal Data Collected by Third Parties regulates and controls the informed and rightful treatment of personal information including the ARCO rights which are, the rights of Access, Rectification, Cancellation and Objection [7]. According to an assessment made in this country to 734 internet

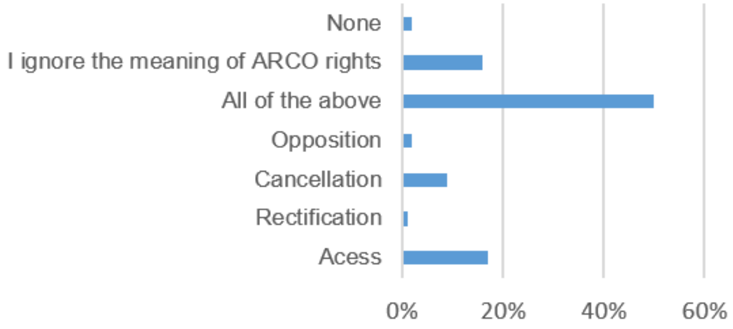

Fig. 2. Assessment made to consider ARCO rights by [1]

users by the Internet Mexican Association (IMIPCI) [1] a 5 out of 10 assessed consider ARCO rights to be very important (see Figure 2).

2.3 Are People Worried about Privacy?

Every time someone creates an account to access an online service it requires some information like name, birth date, the city of residence, etc. People are used to giving that information away very easily in exchange for the service they want. It is a normal process that is not considered as disclosing their privacy to third parties. Based on the same study [1], it turned out that 89% of the interviewed people do not think the right to privacy is a constitutional right. Some other highlights are that only 19% take the time to read the privacy notices which have an estimated reading time of roughly 5 minutes. Just 4% of the internet users assessed understand the objective of the privacy notice and 31% of the persons could not define what personal data is, neither 28% of 187 of the companies evaluated.

This comes as a surprise considering that 90% of the assessed companies admitted collecting personal information. Figure 2 illustrates the most common sites where personal information (including sensitive data) is freely given by users [1]. Social networks, online banking, and online shopping are the top 3. In a different question, “What type of personal data have you provided?”, almost 4 out of every 10 internet users admitted to having provided sensitive data and 9 out of every 10 have provided identification data. This shows how most people are not reading their data treatment before using on-line services or platforms, most likely because they do not even believe that privacy is a constitutional right that must be protected, nor are they knowledgeable about which information is considered sensitive or personal and how it can be misused by third parties.

2.4 Privacy in Social Networks and IoT

Social networks imply an important risk regarding the privacy of personal information. In Mexico, 9 out of 10 internet users have access to a social network profile. The small fraction remaining do not access these services because they care about how their private personal information is shared. Such concerns have increased recently [1].

Most on-line social network users have enabled the privacy settings offered, however, 61% do not know how their data is managed, and 3 out of 10 consider that are not in control of the information shared on this platforms. Nevertheless, when questioned if they “agreed to sharing personal information with millions of persons without any restrictions?” there were 35% of internet users who completely agreed; leaving the responsibility of managing their personal data to others [1].

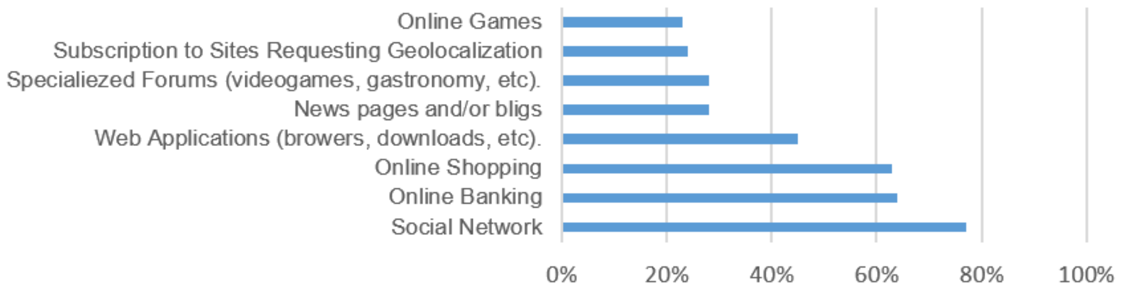

Fig. 3. Most common places where people share their personal information by [1]

3 Ignorance Makes You Vulnerable and Leaves You Exposed

The Mexican people are rapidly becoming internet users [1, 8] and they should know their privacy rights and how to protect themselves from being a victim of private data treatment and theft. The risks of access to private information that the IoT has brought seem to take most users by surprise, mainly because of ignorance or unawareness. Currently, 19-28% of internet users have been active in on-line healthcare discussions and search engines. A significant amount of Protected Health Information (PHI) (see Table 1) can be found on web hubs (e.g., microblogs, online forums, social networks). Surveys of medical forums revealed that personal accounts add up to 49% of the participants, whereas only 25% of visitors are motivated by the usefulness of their content.

People do not realize about the risk they are exposed to when 40% of the world population can freely access this information. PHI leaks can be done by combining Software Engineering (SE), Natural Language (NL) and Machine Learning (ML), mining or harvesting from messages to further use and abuse the privacy of individuals. It is needed to improve guidelines for users to avoid excessive PHI disclosure in on-line posts. Knowledge about the dangers of sharing sensitive information is the most powerful tool to protect it [24].

Rumors and urban legends describe vast disk farms in basements near Washington, D.C. archiving every email, web page change, Usenet postings and even conversations by VoIP telephony. Internet users in China experience strange delays and “page not found” messages that lead them to believe they are being watched online. Many governments have done some form of clandestine monitoring of the Internet” [12] . This information is not stored just by the authorities but by individuals whether they are just curious or malicious about it.

Not only can information be stolen directly from the Internet, it can even be stolen from a discarded personal device. Simply deleting a file from a computer may not completely erase the data from the machine’s disk system. When first using a smartphone with internet access an email account must be used to log in, allowing the use of a variety of features to make lives “easier” by collecting information, processing it and sharing it at its convenience from one feature/device to another, including information “deleted” from the device.

3.1 What Are the Applications that Provide Information about Us?

Users probably ask themselves what information are they currently providing through the applications they have installed on their smartphones. These may include the simplest maps app that gives access to the current traffic and the shortest or fastest route to frequent visited places that are tagged as “home”, “work”, “school” and others, saving some time. Or tools that stamp every single photo taken with properties not just about the time and date, but also the city and street.

And smart TVs that record viewing habits and preferences, as well as devices which monitor

Table 1. Some information health by [24]

N°	Information
1	Names
2	All geographical subdivisions smaller than State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code.
3	Dates (other than year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89.
4	Phone, fax, SSN, medical record, account, certificate/license and plate numbers.
6	Electronic mail address
13	Device identifiers and serial numbers
14	Wen Uniform Resource Locators (URLs)
15	Internet Protocol (IP) address numbers.
16	Biometric identifiers, including finger, retinal or voice prints.
17	Full face photographic images and comparables images. Etc.

the presence of family members through smart alarm systems, etc. In this context, social media accounts and profiles cannot be ignored, as through them feelings, activities, tastes in music, food, or places visited, and -most importantly- relations and interactions with other users are shared, offering acces to personal networks and an endless supply of fresh data.

4 How Worried Should We be About Someone Else Having Access to our Private Life?

Considering that “the frequent, simplistic response is ’I am not worried about privacy. I do not have anything to hide.’ While there is much to be said for openness and transparency, they can nevertheless be over-rated and are seldom uncomplicated” [3].

“There are massive sets of data now being created for a variety of potentially justifiable reasons: phone logs revealing calling patterns, genetic makeup of individuals, voter lists, credit card purchases, shopping patterns..., the list is long and impressive” [3]. So, what make us think that we are not vulnerable and that our kids are not vulnerable either where not just people itself but also companies are being victimized of large data breaches and inadvertent data leaks with 2,164 incidents reported in 2013 [23].

4.1 Kids Are the Most Vulnerable in the IoT?

“Any sort of hurtful or dangerous behaviors that occurs between minors offline can now occur on-line (i.e, bullying, gossiping, ostracizing, harassing, encouraging each other to engage in risk taking -sexual or otherwise-). Indeed, many consider cyberbullying the number one threat to children on-line. Finally, there are threats to children’s privacy and reputation on-line. The differences between the on-line and off-line world make children’s on-line communications particularly vulnerable to invasions of privacy or the inadvertent revelation of sensitive or potentially embarrassing information” [20].

Danah Boyd [4] has argued that there are features of social networks that make them a greater threat to privacy than off-line communication. Most notably, unlike talking with a friend in person or on the phone, on-line communications are recorded; they are, thus, persistent, searchable, and copy-able. Furthermore, we have much less control over who can access this communication and these features of on-line communications make them a serious threat to privacy.

Alice Marwick et al. [13] point out, “Once digitized, such information is virtually irretrievable and may be intercepted or purchased by commercial entities, governments, or individuals for marketing or other more sinister purposes”. The privacy threads affects everyone, but children are particularly vulnerable because of the ignorance about what is private information and the consequences of sharing it and which is even worst is the fact of these behaviors follow them into adulthood having a serious long term impact on their lives.

It is well known that despite of all the dangers hanging in the internet there is also a world of possibilities for e-learning, civic participation, leisure, creativity, social interaction and self-expression. But unfortunately, the risks they face there go from cyberbullying, to being exposed to violent, hateful, anti-social, or sexual content, being targeted by advertisers, and unwanted sexual solicitation. We need to make anything that is in our hands to minimize the impact and exposure.

4.1.1 Is it Necessary and Correct to Monitor the Kids?

Parents that are open with their kids that they are monitoring internet information exchanges have the value of honesty but this can lead to monitoring escape actions from the children since according to a survey made to children 9-17 years old in Britain, 69% said that they mind their parents monitoring or restricting the internet access, 63% of 12-19-year-old said that they took some action to protect the privacy of their on-line information exchanges from their parents [8].

In a research done by K. Mathiesen [15] is said that not only adults but also children have their personal information vulnerable and it has been recommended that parents should monitor their kid´s internet usage, including messages they receive, sites they visit, what they post, etc. But in case parents follow this advice would not their children´s privacy rights being violated?

“The advice to monitor comes from a desire to allowing children to go on-line while trying to protect them from possible harm at the same time from some of the risks mentioned above or even greater concern is the possible harm that children may be exposed to when they interact with others online. There are frequent worrying reports about “Internet predators” (i.e. pedophiles who may begin by contacting minors on-line, solicit photos or engage in inappropriate communications, and perhaps go so far as to convince the child to meet in person)”.

Common advice examples for parents include to search for the web history, review what is on their computers, using software that monitor their Facebook entries, posts, contents looking for questionable and potentially dangerous content. In fact, 77% of the interviewed parents in the U.S. have done one of this, against 50% in U.K. Whether it is performed as a covert or overt practice this monitoring action has been considered or associated with good parenting.

Are they right about this privacy violation? Well, the United States legal system do not think that. However, the fact that is not illegal does not make it ethically correct. Alice Marwick [13] defends the fact of being “ethically inappropriate to advise parents to monitor. Because, when children engage in informational exchanges with others, their privacy ought to be respected (even by their parents). Informational exchanges can be defined as conversing, Internet searching, reading books, articles, or updates, blogging, posting or viewing photos or videos, etc”. There are three objections stated against the paternalistic arguments of monitoring.

Risks are over stated is the first one, where “some argue that the discourse surrounding children and the Internet is a ’technopanic’. A ’technopanic’, according to Alice Marwick [13], ’manifests itself to modify or regulate young people’s behavior, either by controlling Young people or the creators or producers of media products’ ”. One might think that the advice of monitoring children´s Internet usage is merely a symptom of this “technopanic”. And in fact, the empirical evidence shows that the level of risk is frequently overstated since it has not been proved that monitoring minimizes the risks. Others argument against the need for monitoring stating that “it is just information” but we should not forget that Information itself is inert just without our responding interpretations, beliefs, and actions.

The monitoring is ineffective is the second argument where we believe in the ineffectiveness of monitoring as a method for protecting children, because we cannot infer someone’s believes and intentions from what information exchanges that person. You can say you did something for everyone to read it, but that does not mean it is true.

The monitoring may lead to harm is the last argument. “The effectiveness of monitoring might further be called into question, because, even in cases where parents gain true and useful information from monitoring, parent’s response to this information may be harmful to the child”.

Depending on the parent's education and religion realizing about the online searches their children do (i.e., "I think I am gay") where they expose their fears and doubts and trying to look for responses, the reaction may not be the best for them and can lead to be more harmful than any other online danger.

However, these does not mean that monitoring may not be helpful in other cases where parents use the information gained in ways that would be beneficial for the child but even if parents are able to protect them from some hazards by monitoring their kids´ information, they ought not to do so. The right to keep their information exchanges private is also for the children. Parental obligation is to respect it, and it is grounded in two normative considerations which considers first fostering their current and future capacities of autonomy - a being capable of making choices in light of self-determined preferences and moral norms. And second of al is related to their current and future capacities for relationships (several philosophers have argued that some degree of privacy is necessary for personal relationships).

4.1.2 Ways to Enhance On-line Safety without Violating Privacy

The question: how can we let children to fully enjoy and take advantage of the online access media but minimizing the risks of unwanted content such as cyberbullying or unwanted sexual solicitation? Keep people talking about if parents should leave this in hands of legislators? Nevertheless, there is also a more balanced approach that suggest parents to "engage in activities such as talking to their children about Internet content and structure, encouraging children to explore the Internet, sitting with them or nearby while they go on-line, and sharing online activities" [11].

"While one approach may not fit all, it has been shown that social co-use reduces risk regardless of differences in child-rearing culture" [11]. "If parents encourage open communication about on-line activities to start with, children may be more likely to discuss troubling experiences with their parents. As noted above, monitoring tends to undermine trust and, thus, to undermine children's voluntary sharing of information" [11].

4.1.3 Do Parents in Mexico Monitor their Kids?

Vying towards an accurate comprehension of the monitoring phenomenon within the Mexican context, 151 semi-structured surveys (comprising 14 closed and 7 open questions) (see Table 2) were conducted to Mexican parents with children between 5 and 17 years of age. during the month of May 2018. The age ranges selected are based on those used by the Asociación de Internet.mx (formerly AMIPCI) [1], which differentiates age groups in children between those that are 6-11 years old and those between 12-17 years old. However, these ranges were broken into smaller groups and it was decided that 5 year olds should be included as well. The people surveyed remained between 27 and 56 years of age, comprising 69.5% women and 30.5% men. Regarding the children, 24.36% correspond to 5-7 year old, 18.91% to 8-11 year old, 24.36% to 12-15 year old, and 32.36% to 16-17 year old teenagers.

The answers regarding the age at which children began to use the Internet, show a wide range from 1 year old to 13 year old. It can be inferred that the delay of the start is connected to the evolution of technological devices, their penetration among the population, as well as their quality. Thus, the younger the parents are, the lower the age at which their children are allowed to use devices with Internet Access. However, even in cases with parents older than 48 years of age, with children aged 7 or younger the same situation arises, with which it can be argued that the decision to allow access to young children (5 years or less) to these devices does not necessarily depend on generational values, but on the availability and accessibility to technology which has allowed a greater adoption rate as time goes by.

On other hand, the most common connection device turned out to be smartphones owned by the children (32.6%), followed by smartphones owned by the parents themselves (20.6%). For younger parents, the devices of choice are tablet computers owned by the child (17%) and smart TVs (9.2%), although there are some cases where children 7 or

Table 2. Example of semi-structured surveys

N°	QUESTION	RESPONSE OPTIONS
1.	Are you?	Mother Father
2.	Your age?	*open question
3.	What is the age range of your children?	*open question
4.	At what age does your child start using devices with an internet connection?	*open question
5.	What is the device they use the most?	Smartphone (child property) Smartphone (parent property) Tablet/iPad (child property) Tablet/iPad (parent property) Laptop (child property) Laptop (parent property) Desktop computer (child property) Desktop computer (parent property) Smart TV Video game console
6.	How much time a day does your child stay online?	*open question
7.	Do your children have personal profiles on social networks?	Yes No I do not know
8.	If your answer is yes, do you know the privacy terms of social media platforms?	Yes No
9.	Do you monitor your children's activity on the internet?	Always Regularly
10.	Only when I detect something abnormal	Only when I detect something unusual I do not consider it necessary
11.	In the case of applying, in what way do you carry out the monitoring?	*open question
12.	Do you have rules for internet use for your children?	Yes No
13.	Do you use parental control systems?	Yes No I do not know

younger use their own smartphones. It might be inferred that young parents choose to expose their children to the Internet through Tablet computers and television to capture their attention in the form of entertainment and leisure, freeing time for the parents to take on other activities.

Regarding the time spent on-line, there is apparently no trend defined by age, as it was not possible to establish a range which implied a certain increase in the amount of time spent connected to the Internet. Although it could be expected to find a relation between children of school age and the time needed to perform research tasks on-line, the data shows instances where parents of children as young as 5 years old and as old as 17, answered that they remained connected throughout the day, with no considerable variations for the rest of the age ranges.

It should be mentioned that only 4.3% of parents with children between the ages of 8 and 15 answered that they are unaware if their children have profiles on social networks, while 49.6% confirmed that they do have them. Interestingly, most children with personal profile pages at social networks for the range of 5 to 7 year olds match those cases of children who started using Internet devices from 2 to 4 years of age. Eventhough, 49.6% parents know that their children in the age bracket from 8 to 15 years old have profiles in social networks, only 34.3% consider that they know the terms of privacy of such platforms; however, it should be noted that there is no certainty that the people surveyed are indeed familiar with said terms of privacy of the major social networks and digital platforms.

In regards of supervision, 37.6% -mostly mothers of children between 5 and 7 years of age- stated that they always monitor their children's activity on-line. 29.8% of all parents monitored their children's regularly without observing a trend by age range, as is the case of 17.7% that only does so when something abnormal is detected. Alarmingly, as much as 14.9% of parents of 16 and 17 year olds admitted not to do it because they do not consider it necessary. 54.26% of those parents who actively monitor their children's activity on-line choose to check their search history or to be privy to their children's passwords for smartphones and social networks, while 15.96% stated that their children are only allowed to use devices with access to the Internet, while in their presence. Almost 13% of parents follow their children on social networks and monitors their public activity, friendships, activities, interests and other types of interaction on-line. Only 7.45% use parental control tools or have their children's accounts linked to their smartphones, while only 4.26% blocks specific pages.

Even though, as little as 5.32% ask their children directly about their on-line activity, most parents go through their browsing history which, ironically, as the literature review suggests, implies an invasion of the child's privacy.

This highlights the small amount of parents who prefer to use communication and trust to talk directly with their children because a good communication is more effective than invasive monitoring. The survey shows that 73.8% of parents have established rules of internet use for their children, while the remaining 26.2% that have not correspond directly to the parents of teenagers aged 16 to 17.

Although most cases have established rules, these do not match with those who champion communication with their children, so the effectiveness of these at minimizing risk can be questioned considering they mostly miss reinforcement through the generation of confidence scenarios. It can be inferred that most parents would assume that by the age of 16, the child has enough discretion not to expose their privacy or not to be endangered on-line. On the other hand, although some parents do not admit to having internet usage rules, they leave the decision making to certain algorithms since 43.2% of the parents declared to use parental control systems.

This shows a paradoxical trend where technology is in charge of the protection of privacy and the avoidance of risks to which minors are exposed due to the same technology. It most be noted that as much as 46% of the parents surveyed do not use any parental control tools and that an alarming 10.8% does not even know what a parental control system or if it is being used, which represents a risk in itself, especially for the younger population.

Those parents who have experienced some problem with their children because of their use of the Internet, admitted to monitoring their children's on-line activity "always" or "regularly". This reinforces the position that invasive monitoring is not directly related to the minimization of risks. Given the ages of those involved, it is observed that by using private spaces (bedroom) to connect to the internet, not having Internet usage rules, and having access to basic knowledge of how to hide browsing and search history records from their parents, they become the most exposed population. On the other hand, it is interesting to notice that connecting to the Internet from shared spaces at their homes, such as living or dining rooms, under the gaze of their relatives, has not avoided the risk of having problems on-line.

Regarding their activities, 67.4% of parents consider that the main use that children have fot the internet has to do with leisure activities, games and social networks, and only 29.8% thinks it is linked mainly to information searches for schoolwork. However, most parents (69.05%) consider that the main benefit gained by their children connecting to the Internet is access to information useful for their learning, while 19.05% consider that the advantages have to do with leisure and entertainment and 11.9% with communication.

44.19% of parents agree that the main danger to which their children are exposed while on-line, is access to violent and sexual content, followed by 15.12% who think it is its potential contact with dangerous strangers. With regard to this, 12.79% consider kidnapping and extortion a serious risk. While 9.3% distrust social networks and so-called ”influencers” as questionable role models, 6.98% fear theft through deception, 5.81% fear harassment and bullying to the same extent as identity theft. The issue of privacy is rarely considered. A great share of mothers appear to be more aware of the dangers of exposure to sexual content, while fathers are afraid of contact with strangers who can potentially harm through kidnapping or information theft. Parents of younger children are more concerned with exposure to sexual content, while the parents of teenagers fear peer pressure, vices, kidnapping and information theft.

Finally, 70.2% of parents acknowledge they are aware of the logging of data, on-line activity and preferences of their children, through the platforms they visit or applications they download. However, most admit to only 34.3% skimming through Privacy Terms and Conditions, keeping in line with the little attention they give to privacy issues while ranking data, information and identity theft as potential dangers. Thus, 36.9% said that they do not mind the logging and tracking of their children's on-line activity. because “there is nothing to hide”; 33.3% reviewed the Terms of Privacy of platforms and applications that their children use; while 26.2% stated that even though they are concerned, that is how the Internet works and there is nothing they can not do about it.

5 Security Measures to Safeguard your Privacy

No matter what the purpose of any application or device is, these were designed and created from humans to interact or provide a service to people. This fact makes vulnerable not just the systems but also the users, as we had commented before, being the weakest link in the chain.

They are a perfect target. For this reason, it is important for them to know the existing threads and how to avoid them. It means that Information Security Education is needed for every Internet user.

Below there is a guide that based on all the research has become a proposed reference guide for any user that wishes to have data protection level (let is not forget that we will never be 100% secure, but as many locks, we set the more difficult it will be to break them up).

5.1 Non-Technical Security Measures

Use common sense even if computer knowledge is limited. Many parents do not know anything or just know a little about computers, however, the age brings us common sense, something that the kids may not possess yet; a thing that can be used in our favor to avoid conducts that may put them in risk. We must talk to them about the same life principles/rules we follow in the real world like “Do not talk with strangers!” (and follow it yourself as a parent also, be the example), remember that virtual world is real too. Let´s remember that there are predators online that may want to blackmail us, or a cyberbullying may be occurring.

Instruct yourself about how social networks work and tell the kids that not all the online content is true, do not be an easy prey. It is easy to steal private information directly to the owner, no hacking needed, with social engineering. Educate ourselves and transmit to the children good practices such as not sharing any personal information (phone number, address, location, school, etc.) and tell them why. Think twice what you are going to post online, does it have personal or compromising information? Is the question to be asked, if yes, do not post it. Make sure that photo you are about to share is not compromising. Who is in the photograph? What does the picture tell about the people there? Is it compromising? if you agree it is ok, post it.

Read the privacy policy of the sites and apps you use, including the cloud. It is rarely done, but highly recommended to know what data is going to be collected and how is going to be treated. Do not use social logins on untrusted sites. As adults and kids, we love plays, quizzes and surveys taken online specially on Facebook where we logged in and give permission to access our profile and our friend's information in order to be able to see the results. All the collected information is used by a third-party company for targeted advertisements and perhaps something else, who knows.

Hence, using fake personal information like birthday on Facebook, if you use one at all, or first and middle name is preferable. Do not connect your devices unless you need to. Just because the TV, the fridge or that beautiful toy can connect to the internet, does not mean you have to. Investigate about the functions they offer on-line and off-line to see if is worth it.

Transmit trust to the children. This is important, open communication channels with the whole family, so the security education can be transmitted, and you can realize if something is going on and everyone can feel free to tell it. Follow and friend your kids for a better follow up of the people they have listed as friends and see if there is anyone suspicious and does not forget to explain the risk and dangers.

Keep an eye on their behaviors. The trust is not always enough; there are plenty of factors that can make them do not tell if a menace is going on, there is where the common sense, trust and well known of the children behaviors take place to act. Certain children use the social networks profiles that you know, but not everyone. Do not be overprotective with the children nor anyone so they do not have to hide anything from you, make them trust you. Locate the computer in a visible place this can minimize risks since you are more aware of what it is been done without his meaning lowering the user's privacy.

5.2 Technical Security Measures

Always use authentication mode (more than one is recommended) for all the devices you own, and preferably more than a simple password, fingerprint and facial and/or voice recognition (biometrics) are also examples of it.

Do not use the same password for all the accounts, nor reuse them, and never leave the default password. The email security is important since many other accounts are related to this one and can be reset, deleted, etc. from there. It is recommended to use a different email account to connect to these devices when needed, one where no emails are expected.

Make a strong password with a capital letter, lower case and special symbols with minimum 10 (but recommended is 25) characters long and try to remember it or you can use a password ID manager to help you store all the passwords. There are many options in the market like LastPass or 1login, make sure to read terms and conditions before.

Implement a full security solution, use a firewall, an antivirus, an antispyware or malware and keep them up to date, do not forge to continuously scan your computer. These mechanisms will make it harder for anyone trying to do so. There are more complete solutions nowadays for smart homes, like Norton, that protect the entire network and all the devices connected to it but not just a specific one.

Back up your information, this can be on an external hard drive, a DVD or in the cloud (read privacy statement before). In case of stolen information, this will help you a lot to recover them easily, preferably encrypt it.

It is important to apply the Operating System updates - patches and fixes (Windows, Linux, Mac OS, etc.) since they have the "vaccine" for vulnerabilities discovered that could be exploited if you keep an old-fashioned OS. This can be usually done by going directly to the company´s official site or in the settings and update section on the device.

It is strongly suggested to do not connect the devices in public WIFI connections, if needed, opt for a Virtual Private Network. In addition, at home, create a separate network especially to connect IoT devices that have questionable security, so they do not "live" in the same space as your shared filed or other networked devices. Many Wi-Fi routers come with the "guest networking" function available.

Go to the settings options and turn off Universal Plug and Play (UPnP) protocol that makes routers, cameras, Smart Tv´s and other devices vulnerable.

Disable apps for starting automatically and make sure your browser does not remember your passwords, otherwise, this can lead you to be a victim or even better, search anonymously, whether, for homework or curiosity, children will need to use search engines. Many search engines will collect information on every user and build a profile for targeted ads.

The recommendation is to use different search engines that do not log information such as IP Addresses, cookies or monitor what is been clicked like DuckDuckGo, StartPage, and ixquick. Disable the features such as Bluetooth, WIFI, NFC and GPS. Adjust the privacy setting of all the social network accounts and make the profiles just visible for trusted people and remove the accounts from search results so strangers can not send friend requests.

Do not make banking transactions nor online shopping in sites that not include a secure connection with HTTPS (there is a little lock next to the URL). Websites that do not use security certificates put our information in danger since it is being sent in text plain and anyone sniffing on the network can easily get to it and steal it. However, if a secure web page is selected our information will travel among the network encrypted and this will be unreadable.

Disable the WEP configuration from the routers/modems; change it to a stronger method as WPA2. The vulnerability was found in WEP method, now there are applications that can “guess” the password of connections like that.

If you are sending something make sure it is the right email address or direction. You do not want to send personal information to the wrong person.

Only download application from trusted sites (app store and play store). These sites follow a research process for the apps they hang in their stores which make us feel a little more secure but remember to check the privacy policy and permissions required for installation before doing it. Be aware of the app functionality and main purpose of it and make sure it is not asking you for extra permissions or accesses during the installation.

5.3 Parental Controls and Software

The use of the Parental software is suggested to regulate internet access to websites (but this is merely a suggestion and parents may agree or disagree with this practice).

Depending on the Operating System is the amount of parental controls that are available as a built-in function. For example, Android devices lack dedicated parental control but some come with the ability to create multiple user accounts. In the settings, check for a “Users” section, where you can add a restricted profile managing the apps the kids can use. As for iOS devices, unlike Android, they are easier to monitor and manage what kids do you can turn the geo-location off, n-app purchases can all be turned off or filtered, social media and location services can be restricted, disable installed apps and certain features, click on Restrictions and create a passcode.

For more granularity or micromanagement there are plenty of parental control apps out there in the market with really cool features and dashboards that allow the parents to control not just what the kids are able to access applications and websites but also set the specific time when these devices can be used and for how long, are capable to detect and prevent the child to share any kind personal information and even a GPS-based location monitoring to know where are the kids (assuming the cell phone is with them) all the time.

There are some free and premium options available in the market right now depending on what the parents are looking for, how many “cool” features are needed. As premium alternatives, we have Qustodio, Net Nanny, and PhoneSherriff, OurPact, and Kidslox fluctuating around $49.00 USD. But there are also a few free choices like Funamo, Lock2Learn, MM Guardian, and AppLock.

6 Conclusions

As discussed, ignorance or lack of knowledge in certain areas makes people the weakest link in the process of private information management, because what is unknown cannot be avoided. Certainly, education is meant for empowering people to help them develop in different areas of their lives. Development cannot happen without education. Hence, according to the United Nations [18], all human beings should have access to at least basic quality education; and communities around the globe had acknowledged the fact and had produced political demands about it.

Assessing what the United Nations states, it might be questioned that if education empowers people and that basic education is a right for all human beings, why should not that be the starting point? Why should not information security education start on a basic school level? Basic, or elementary school is a gateway towards social life, where the toolbox for interaction is shaped, Should not it consider the basic guidelines to survive and to thrive in the environment of on-line social networks and the IoT, as well?

However, as important as it is to share non-technical suggestions to rise awareness, as it is to implement technical measures that will help to avoid some risks and hazards of on-line activity, it is necessary to acknowledge that such recommendations are useless if people do not understand the broad range of issues they are exposed to. There is where both guidelines merge: there are important non-technical issues that need to be addressed for any proposed technical solution to work properly.

The Internet Mexican Association states that the average age for children to start using the internet is 8 years old, [1] that means that the Information Security and Privacy gap should be covered before that time frame, tending to those who are about to become users. If they are educated about what constitute personal information, why it is protection is paramount, who may be interested in acquiring it and the different strategies that those third parties and even people we know might use it wrongfully, it would mitigate at the very least make it difficult for the children's privacy to be compromised.

The ideas discussed hereby have the potential to inform a comprehensive project for elementary Information Security and Privacy education in places like Mexico where the number of Internet users is growing every year [1]. This project should not be geared just towards children, it should consider the importance of trust and dialogue amongst families. The spread of such information would likely have an impact on Internet habits and trends, reducing data leaks, and improving the awareness of the risks and hazards of on-line experience.

Designing the seed of a solid, well informed, culture of Information Security and Privacy in elementary schools is quite challenging; it would comprise the investment of considerable time and resources to make it happen, such as a network of interested people and institutions and an objective account of the results of its benefits and impact.

References

1. **Asociación de Internet (2018).** 14 Estudio sobre los Hábitos de los usuarios de Internet en México 2018.
2. **Atzori, L., Iera, A., & Morabito, G. (2010).** The Internet of Things: A survey. *Computer Networks*, Vol. 54, No. 15, pp. 2787–2805.
3. **Bird, S. J. (2013).** Security and Privacy: Why Privacy Matters. *Science and Engineering Ethics*, Vol. 19, No. 3, pp. 669–671.
4. **Boyd, D. (2008).** *Youth, identity, and digital media*, chapter Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life. The MIT Press, pp. 119–142.
5. **Cambridge (2018).** Cambridge Dictionary.
6. **Chabridon, S., Laborde, R., Desprats, T., Oglaza, A., Marie, P., & Marquez, S. M. (2014).** A survey on addressing privacy together with quality of context for context management in the Internet of Things. *Annals of telecommunications*, Vol. 69, pp. 47–62.
7. **General Congress of the United Mexican States (2010).** Federal law of personal data held by third parties.
8. **INEGI (2015).** National Survey on Availability and Use of Information Technologies in Households (endutih).
9. **International Telecommunication Union (2005).** *The Internet of Things*. International Telecommunication Union, 7 edition.
10. **Keenan, T. P. (2007).** *The Future of Identity in the Information Society*, chapter On the Internet, Things Never Go Away Completely. Springer, pp. 37–50.

11. **Kirwil, L. (2009).** Parental Mediation Of Children's Internet Use In Different European Countries. *Journal of Children and Media*, Vol. 3, No. 4, pp. 394–409.

12. **Langheinrich, M. (2009).** *Ubiquitous Computing*, chapter Privacy in Ubiquitos Computing. Chapman & Hall / CRC Press, pp. 1–44.

13. **Marwick, A. E. (2008).** To catch a predator? the MySpace moral panic.

14. **Marx, G. T. (2001).** Murky conceptual waters: The public and the private. *Ethics and Information Technology*, Vol. 3, No. 3, pp. 157–169.

15. **Mathiesen, K. (2012).** The internet, children, and privacy: The case against parental monitoring. *SSRN*, Vol. 2012, pp. 1–22.

16. **Miorandia, D., Sicari, S., Pellegrini, F. D., & Chlamtac, I. (2012).** Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, Vol. 10, No. 7, pp. 1497–1516.

17. **Morgan, J. (2014).** A simple explanation of 'The Internet of Things'.

18. **NATIONS, U. (2000).** Education.

19. **Oxford (2018).** Oxford living dictionaries.

20. **Patchin, J. W. & Hinduja, S. (2006).** Bullies move beyond the schoolyard a preliminary look at cyberbullying. *Youth Violence and Juvenile Justice*, Vol. 4, No. 2, pp. 148–169.

21. **Research & Markets (2013).** Internet of Things (IoT) & machine-to-machine (m2m) communication market - advanced technologies, future cities & adoption trends, roadmaps & worldwide forecasts (2012 - 2017). Technical report, PRNewswire.

22. **Roman, R., Najera, P., & Lopez, J. (2011).** Securing the Internet of Things. *IEEE Computer*, Vol. 44, No. 9, pp. 51–58.

23. **Sokolova, M. & Matwin, S. (2015).** *Challenges in Computational Statistics and Data Mining*, chapter Personal Privacy Protection in Time of Big Data. Springer, pp. 365–380.

24. **Tsai, C.-W., Lai, C.-F., & Vasilakos, A. V. (2014).** Future Internet of Things: open issues and challenges. *Wireless Networks*, Vol. 20, No. 8, pp. 2201–2217.

25. **Warren, S. D. & Brandeis, L. D. (1890).** The right to privacy. *Harvard Law Review*, Vol. 4, No. 5, pp. 193–220.

Article received on 12/04/2018; accepted on 12/07/2018.
Corresponding author is Maria G. Vallejo.