8-11-2017

Towards a Privacy Rule Conceptual Model for Smart Toys

Laura Rafferty

Patrick C. K. Hung

Marcelo Fantinato

Sarajane Marques Peres

Farkhund Iqbal

See next page for additional authors

Recommended Citation

Rafferty, Laura; Hung, Patrick C. K.; Fantinato, Marcelo; Peres, Sarajane Marques; Iqbal, Farkhund; Kuo, Sy-Yen; and Huang, Shih-Chia, "Towards a Privacy Rule Conceptual Model for Smart Toys" (2017). *All Works*. 3701.
https://zuscholars.zu.ac.ae/works/3701

Author First name, Last name, Institution
Laura Rafferty, Patrick C. K. Hung, Marcelo Fantinato, Sarajane Marques Peres, Farkhund Iqbal, Sy-Yen Kuo, and Shih-Chia Huang

Towards a Privacy Rule Conceptual Model for Smart Toys

Laura Rafferty[1], Patrick C. K. Hung[1,5], Marcelo Fantinato[2], Sarajane Marques Peres[2]
Farkhund Iqbal[3], Sy-Yen Kuo[4], Shih-Chia Huang[5]
[1]Faculty of Business and IT, University of Ontario Institute of Technology, Canada
[2]School of Arts, Sciences and Humanities, University of São Paulo, Brazil
[3]College of Technological Innovation, Zayed University, UAE
[4]Department of Electrical Engineering, National Taiwan University, Taiwan
[5]Department of Electronic Engineering, National Taipei University of Technology, Taiwan
{laura.rafferty, patrick.hung}@uoit.ca; {m.fantinato, sarajane}@usp.br
farkhund.iqbal@zu.ac.ae; sykuo@ntu.edu.tw; schuang@ntut.edu.tw

Abstract

A smart toy is defined as a device consisting of a physical toy component that connects to one or more toy computing services to facilitate gameplay in the cloud through networking and sensory technologies to enhance the functionality of a traditional toy. A smart toy in this context can be effectively considered an Internet of Things (IoT) with Artificial Intelligence (AI) which can provide Augmented Reality (AR) experiences to users. In this paper, the first assumption is that children do not understand the concept of privacy and the children do not know how to protect themselves online, especially in a social media and cloud environment. The second assumption is that children may disclose private information to smart toys and not be aware of the possible consequences and liabilities. This paper presents a privacy rule conceptual model with the concepts of smart toy, mobile service, device, location, and guidance with related privacy entities: purpose, recipient, obligation, and retention for smart toys. Further the paper also discusses an implementation of the prototype interface with sample scenarios for future research works.

1. Introduction

A toy is an item or product intended for learning or play, which can have various benefits to childhood development. The modern toy industry is comprised of establishments primarily engaged in manufacturing dolls, toys and games. As such a substantial part of human development, toys have continued to maintain a presence in the daily lives of billions of individuals of all ages. While primitive toys included rocks and pinecones, they soon progressed into dolls, stuffed animals and trains. Traditionally, toys have been entirely autonomous and without any processing or networking capabilities to communicate with any other device. While a child user is engaged with a traditional toy, it will collect and store no personal data, and require no reason for concern for a child's privacy. With the introduction of electronic toys with embedded systems, electronic toys can have sensory capabilities, and the ability to collect and store inputted data based on the user's interactions. This data is limited and used only for the interaction, often discarded immediately. An electronic toy has limited or no networking capability. Thus, privacy concerns are limited to nonexistent in this context. In the past few decades, electronic toys such as Speak & Spell, Tamagotchi, and Furby had become popular.

A smart toy has been defined as a device consisting of a physical toy component that connects to one or more toy computing services to facilitate gameplay in the cloud through networking and sensory technologies to enhance the functionality of a traditional toy [1]. A smart toy in this context can be effectively considered an Internet of Things (IoT) with Artificial Intelligence (AI) which can provide Augmented Reality (AR) experiences to users. Examples of these are Mattel's Hello Barbie and Cognitoys' Dino. Smart toys are able to gather data on the context of the user (e.g., time of day, location, weather, etc.) and provide personalized services based on this context data. However, the user may not be comfortable with the level of data that is collected and inferred on them.

There are three general properties of a smart toy: *(1)* pervasive – a smart toy may follow child through everyday activities; *(2)* social – social aspects and multiplayer are becoming a mandatory aspect of interactive smart toys in a one-to-one, one-to-many and many-to-many relations [2]; and *(3)* connected – smart toys may connect and communicate with other toys and services through networks. For example, Cognitoys' Dino can listen and answer questions raised

URI: http://hdl.handle.net/10125/41299
ISBN: 978-0-9981331-0-2

by children by voice because the Dino connected to the IBM Watson's knowledge called Elemental Path's "friendgine", which is a child-friendly database at the backend. Some research studies found out that children have emotional interactions with dolls and stuffed toys in anthropomorphic design [3]. Some children even prefer to take the toy to the dinner table or make a bed for it next to the child's own [4]. Many studies found that anthropomorphic toys such as a teddy bear or bunny serve a specific purpose, as children trusted such designs and felt at ease disclosing private information.

As a result, *Toy Computing* is a recently developing concept which transcends the traditional toy into a new area of computer research using services computing technologies [5]. In this context, a toy is a physical embodiment artifact that acts as a child user interface for toy computing services in cloud. A smart toy can also capture child user's physical activity state (e.g., voice, walking, standing, running, etc.) and store personalized information (e.g., location, activity pattern, etc.) through camera, microphone, Global Positioning System (GPS), and various sensors such as facial recognition or sound detection. In 2015, a new invention called the "Google Toy," which is an internet-connected teddy bear and bunny, like an anthropomorphic device with speech and face recognition functions that will have the ability to control smart home appliances and devices at home. However, this toy has caused many criticisms from the media as people express concern about privacy breaching and safety issues by Google.

More specifically, the toy makers are confronted with the challenge of better understanding the consumer needs, concerns and exploring the possibility of adopting such data-collected smart toys to rich information interface in this emerging market. For example, many toy designers have been researching the balance between the level of private information a toy collected from a child and the level of personalized features the toy provided to the child. Referring to the direction of the United States Federal Trade Commission Children's Online Privacy Protection Act (COPPA) and the European Union Data Protection Directive (EUDPD), the definition of a child to be an individual under the age of 13 years old. In this paper, the first assumption is that children do not understand the concept of privacy and the children do not know how to protect themselves online, especially in a social media and cloud environment. The second assumption is that children may disclose private information to smart toys and not be aware of the possible consequences and liabilities.

Breaches of privacy can result in threats to the physical safety of the child user [6]. While the parents (or any legal guardians) of a child strive to ensure their child's physical and online safety and privacy, there is no common approach for these parents to control the information flow between their child and the smart toys they interact with [7]. As smart toys are able to collect a variety of data such as text, picture, video, sound, location, and sensing data, this makes the context far more complicated than many other smart devices in particular given that the subjects are mainly children in a physical and social environment. Parental control is a feature in a smart toy for the parents to restrict the content the children can provide to the toy. Though the toy industry has also issued regulations for toy safety, these regulations have no mention of privacy issues in this toy computing paradigm.

This paper presents a privacy rule conceptual model with the concepts of toy, mobile service, device, and guidance with related privacy entities: purpose, recipient, obligation, and retention for the toy computing environment. In this model, the parents/ legal guardians are the owners of their child's data which is collected on their child (the data subject) in according to COPPA and EUDPD. Parents provide consent through access rules which allow their child's data to be shared according to their preferences and privacy compliance. This paper is organized as follows. Section 2 discusses related works and Section 3 presents the conceptual model with related algorithms. Next, Section 4 discusses the model in a prototype interface with example scenarios. Section 5 concludes the paper with future works.

2. Related Work

Recently the topic of smart toy is gaining increasingly more public interest. For example, Yahoo Canada published a report called "Electronic toy maker VTech's zero accountability clause puts onus for hacks on parents" on February 12, 2016, which said: "the collection of data through toys and apps geared towards children presents a growing challenge. In Canada we have a very restrictive and well defined privacy act for the healthcare domain. In the toy industry, they see all those safeguards and guidelines and they only talk about the safety of a toy. Those guidelines have not caught up to the information collecting aspect." This report shows the public concerns on the toy safety and privacy issues in our society. However, there is limited research on this specific cross-disciplinary research topic in toy computing. For example, AlHarthy and Shawkat [8] discuss a security solution to protect the network data from unauthorized access from controlling unmanaged smart devices, but they do not provide a generic privacy rule conceptual model for this paradigm. Next, Armando et al. [9] describe a technical approach to secure the smart device paradigm based on a given organization's security policy, but without discussing the privacy protection model from the perspective of users. Then, Peng et al. [10] present threat detection and mitigation mechanisms on mobile devices in a prioritized defense deployment, but they do not cover a privacy rule model to tackle the requirements of accessing mobile services. Referring to the research works in IoT, Alqassem and Svetinovic [11] describe the challenges to tackling IoT privacy and security requirements as follows: *(1)* it is difficult to determine what information should be protected, when to protect it, and to whom access should be granted/restricted; *(2)* IoT consists of diverse technologies and the integration of these technologies may lead to unknown risks; and *(3)* the changing nature of the environment plays an important role when dealing with the privacy and security vulnerabilities of the IoT. Though there is a lot of related research in security and privacy of IoT, there is no standardized model which focuses on smart toys in this paradigm. For example, Sun et al. [12] proposes a personal privacy protection policy model based on homomorphism encryption in IoT, but there is no specific privacy rule design.

With all of this in mind, privacy is a growing concern among many users of mobile devices. While many users appreciate the value of targeted services in mobile devices, they still express concern over how their data is collected and managed without their knowledge. For example, Cherubini et al. [13] identify privacy as a barrier to the adoption of mobile phone context services. 70% of consumers say it is important to know exactly what personal information is being collected and shared [14], while 92% of users expressed concern about applications collecting personal information without their consent [15]. Mobile applications have adapted countless services to better analyze context data and provide custom services that will bring the most value to a user based on what they are most likely to need. While allowing context data to be collected for services can prove to be of great benefit to users, there is an ongoing tradeoff between utility and privacy [16]. In summary, smart toys which embrace sensory and networking capabilities open up new threats to privacy [17], stimulate new user requirements [18], and establish a unique case for privacy rule model in toy computing. To our best knowledge, there is still no legislation or industry standard which specifically regulates security and privacy requirements for smart toys.

For illustration, the conceptual model we discuss in this paper focuses on how to protect the child's location information based on IETF RFC6280. Referring to IETF RFC6280 by Barnes et al. [19], Geopriv is an Internet Best Current Practice for location and location privacy in internet applications, which enables users to express preferences for the disclosure of their location information. For example, the user can make a rule that their location is not to be disclosed beyond the intended recipient. This architecture binds the privacy rules to the data so that receiving entities are informed of when their data is shared to other parties. Various techniques have been used in attempt to preserve the privacy of a user's location. Some approaches include degrading quality, creating fake location points, uncertainty, pseudonyms, sharing opaque identifiers using symmetric key encryption, k-anonymity through cloaking. Pseudonyms and k-anonymity methods have been proven inadequate for protecting users' location data and preventing re-identification.

On the other hand, location-based services, also known as location-aware mobile services, have become widely popular to provide information such as events, traveling, shopping and entertainment. Location-based services have been defined by Duri et al. [20] as "services in which the location of a person or an object is used to shape or focus the application or service". Pura [21] identifies location as one of the most promising applications of mobile commerce, due to the ability to allow service providers to offer customized services based on context and resulting in increased perceived value and loyalty of customers.

The mobile application industry has observed a widespread adoption of mobile game applications such as Pokemon Go [33]. This has been successful due to factors such as increased mobility and social network integration [22]. Location-based services have also been used in applications for games. The popular mobile game Angry Birds [23] has a location-based feature which allows users to compete with other based on a leader board associated with their location. Next, MyTown [24] is another mobile game, reminiscent of Monopoly, where users can check in to a physical location, buy and sell properties, and collect rent from other players who check into the same location. Then, Kaasinen [25] conducted a study to investigate user needs for location-aware mobile services:

- **Contents**: topical up to date information, comprehensive relevant information, interaction (user is moving and can only provide limited interaction to device), push information based on both location and personalization, detailed search options, planning vs. spontaneity.
- **Personalization**: personal options and contents, user-generated content.
- **Seamless service entities**: consistency, seamless solutions to support the whole user activity.
- **Privacy**: the right to locate, use, store, and forward the location. Privacy requirements are based on legislation and social regulation. The paper also

identifies Platform for Privacy Preferences (P3P) [26] as a potential approach to manage user privacy preferences and compare them to the location-aware service's privacy practices. P3P is a privacy policy framework created by the World Wide Web Consortium (W3C), based on the eXtensible Markup Language (XML), designed to help end users manage their privacy while navigating websites that have differing privacy policies. User's privacy preferences are expressed using A P3P Preference Exchange Language (APPEL), which enables websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by users of P3P browsers. We also adopt the concepts built in P3P into our conceptual model.

3. Privacy Rule Conceptual Model

Privacy rules can be achieved through privacy preserving mechanisms such as access control. In order to provide the most relevant content, the smart toy will need to collect certain context data such as the child's location, and also potential profile information such as age and gender to help determine what their interests may be based on demographic. To gain even more context of the child, the smart toy may collect and retain historical data on the child such as previous movement patterns via GPS, camera and various sensors, to determine where the child is likely to be at certain times, if the child is travelling, or previous interactions with the smart toy such as which content they had previously been interested in. It is clear that the more information is collected on the child, the more relevant services can be provided to the child. However, the user may not be comfortable with the level of data that is collected and inferred on them [27]. There are countless types of data that can be collected from smart toys that must be considered when evaluating the scope of privacy. This is true of collected sensory data, and also from within other applications, sensitive data can be collected such as a user's profile information, contact list, or calendar. All of this information can be collected and analyzed to determine context data about the children and then the smart toy may provide personalized functions [28].

Referring to Figure 1, the children (users) may interact with different smart toys from different toy makers in a physical and social environment such as Mattel's Hello Barbie and Cognitoys' Dino. The smart toys may be equipped with camera, microphone, GPS, and sensors for face and sound detection. These smart toys may send the collected information such as text, picture, video, sound (voice), location and sensing data to the toy computing services, which are published and managed by different toy computing providers and even bind with other third party services, in the cloud. Each smart toy should have its own privacy policy that outlines information including how it will collect, manage, share, and retain the user's personal data [28].

In the privacy rule conceptual model, a subject is a *3-tuple* entity comprised of a smart toy, a device, and a mobile service. The mobile service may communicate with external entities over a network, such as other devices or cloud services. The user who interacts with the subject is a child (data subject) who is associated with an identity and a parent (data owner) who is in control of their data. In this model, access control decisions are based on permissions which are assigned by the parent, comprised of a list of rules for operations (read, write, etc.) and objects. Figure 2 illustrates a core access control model which allows parents to manage their privacy preferences for access to their child's location data, as an illustrative example. In the toy computing environment, location data is particularly sensitive data because it is the location of the child using the toy. The location object is sensitive information when associated with the user's identity since it allows other entities to be aware of the child's physical location. The motivation for this access control model is to protect this property from being shared with untrusted external entities. The motivation for this access control model is to protect this property from being shared with untrusted external entities.

Traditional access control models make access decisions (permit/deny) based on low level operations, such as read and write, for describing a subject's operation on an object. For example, user *A* is allowed to read file *B*, in which case user *A* is the subject, file *B* is the object, and read is the operation. Figure 3 presents an extended access control model for privacy in a toy computing environment. This model shows the privacy access control model extended over top of the core access control model discussed in Figure 2. In the privacy access control model, a request <*Subject, Operation, Object, Purposes, Recipients*> as input, and a response <*Decision, Obligations, Retentions*> as output, as well as an optional acknowledgement <*Subject, Event*> through a communication channel.

In the privacy rule conceptual model, a subject is a *3-tuple* entity comprised of a smart toy, a device, and a mobile service. The mobile service may communicate with external entities over a network, such as other devices or cloud services. The user who interacts with the subject is a child (data subject) who is associated with an identity and a parent (data owner) who is in control of their data. In this model, access control decisions are based on permissions which are assigned by the parent, comprised of a list of rules for operations (read, write, etc.) and objects. Figure 2 illustrates a core access control model which allows parents to

manage their privacy preferences for access to their child's location data, as an illustrative example. In the toy computing environment, location data is particularly sensitive data because it is the location of the child using the toy. The location object is sensitive information when associated with the user's identity since it allows other entities to be aware of the child's physical location. The motivation for this access control model is to protect this property from being shared with untrusted external entities. The motivation for this access control model is to protect this property from being shared with untrusted external entities.

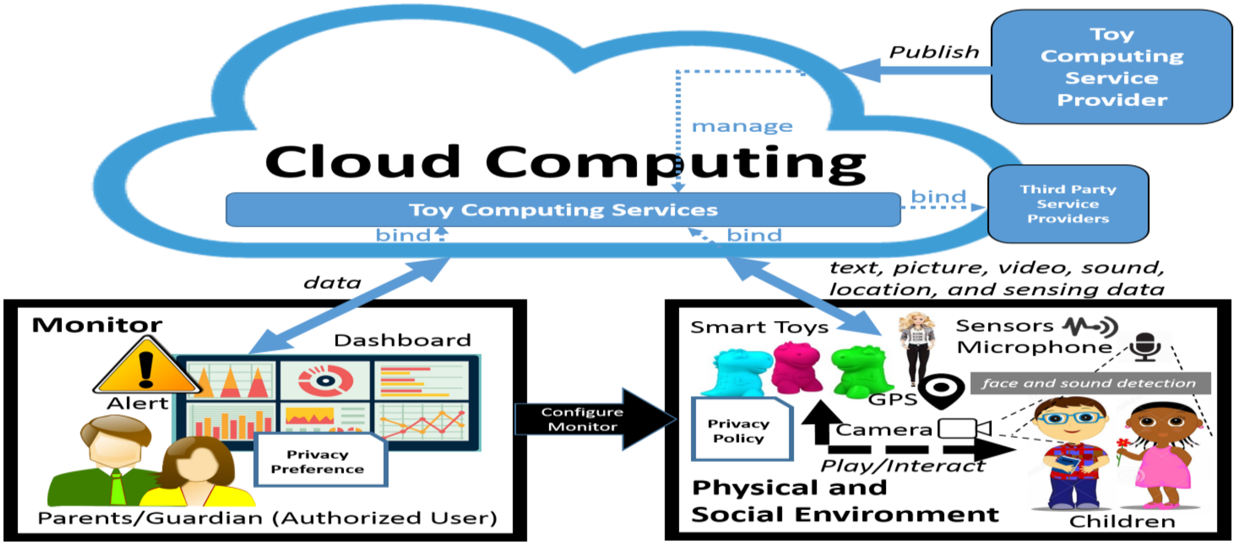


Figure 1. Conceptual Model of Toy Computing

Traditional access control models make access decisions (permit/deny) based on low level operations, such as read and write, for describing a subject's operation on an object. For example, user *A* is allowed to read file *B*, in which case user *A* is the subject, file *B* is the object, and read is the operation. Figure 3 presents an extended access control model for privacy in a toy computing environment. This model shows the privacy access control model extended over top of the core access control model discussed in Figure 2. In the privacy access control model, a request <*Subject, Operation, Object, Purposes, Recipients*> as input, and a response <*Decision, Obligations, Retentions*> as output, as well as an optional acknowledgement <*Subject, Event*> through a communication channel.

In our extension for preserving privacy, we have proposed four privacy-based entities: PURPOSES, RECIPIENTS, OBLIGATIONS and RETENTIONS based on P3P into the model [26] described as follows:

- **PURPOSES:** is a set of purposes in the system. A subject must specify a set of purposes in the corresponding access request. A purpose can be described as different sub-purposes or combined into a general purpose in a hierarchical structure [29]. Figure 4 shows an illustrative hierarchical structure to represent purposes that could be related to toy computing. Different purposes can be generalized as the root element "AnyPurpose", which is the most general purpose in the system. "AnyPurpose" can be subclassified as "Personal Purpose", "MarketingPurpose", "Administrative Purpose", "GamePurpose" and "ResearchPurpose". Each of these can further be subclassified into more specific purposes.
- **RECIPIENTS:** is a set of recipients of the collected object(s) belonging to the subjects/users in the system. Each collected object has a corresponding set of recipients. In the context of toy computing and P3P, recipients can be described as one of the following categories:
  a) ***Individual****:* the subject who made the request or an individual in the system.
  b) ***Group****:* a group of users (e.g., the group of USERS or SUBJECTS currently engaged in a toy computing game session).
  c) ***Third-party***: an entity which does not belong to the system, but is constrained by and accountable to the object owner. This includes EXTERNAL_ENTITIES in Figure 3.
  d) ***Anyone****:* any subject or external entity.
- **OBLIGATIONS:** is a set of obligations in the system that is necessary to be accepted after access permission is granted. The obligations describe the rules that a subject agrees to comply with after gaining the access permission. Obligations are

generally bound to legislation and agreements (e.g., “No disclosure to an unauthorized third party”).

- **RETENTIONS:** is a set of retention policies in the system to be enforced after permission is granted. Each object may have a corresponding retention policy to enforce the duration for how long it may be used or retained. It is recommended that a child’s location data be retained only for the time necessary for the stated purpose. Based on the context of P3P, the retention policy can be described as one of the following categories:
  a) ***No-retention****:* the requested object is not retained for more than a brief period of time, after which it must be destroyed without being logged, archived or stored by the recipients.
  b) ***Stated-purpose***: the requested object is retained for the time required to meet the stated purpose and will be discarded as soon as possible after the purpose is satisfied.
  c) ***Legal-requirement****:* the requested object is retained to meet a stated purpose (as required by law or liability under applicable law).
  d) ***Business-practices****:* the requested object is retained under the stated business practices.
  e) ***Indefinitely***: the requested object is retained for an indeterminate period of time.

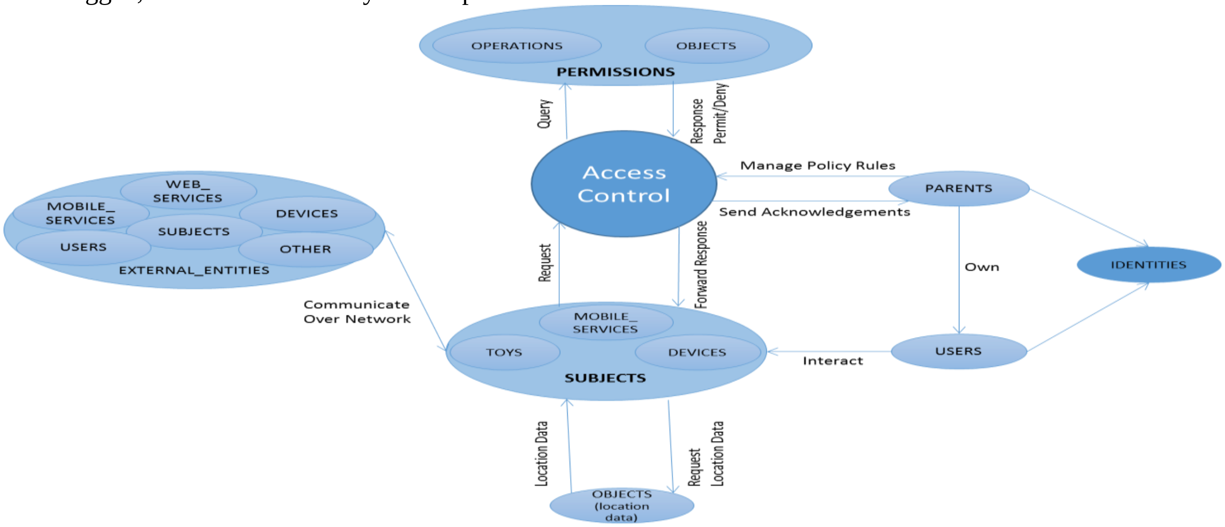


Figure 2. Core Access Control Model

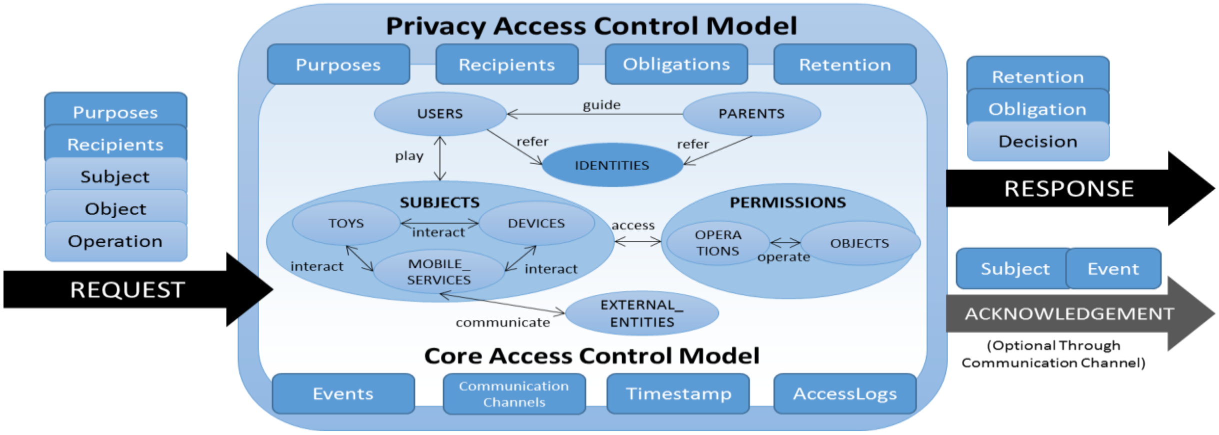


Figure 3. Extended Privacy Access Control Model

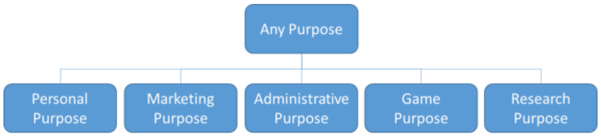


Figure 4. Illustrative Purpose Hierarchy Structure

While we are concerned with location data, some relevant categories are shown in Figure 5 as follows:

a) ***AnyLocationObjectType***: is a general description of any location object type.

b) ***Absolute Location***: is the location expressed in a range or exact GPS coordinates, latitude and longitude. The absolute location can be expressed as coarse (GPS-based, approximate location) or fine (network-based, precise location) [30].

c) ***Relative Location***: is the location relative to another entity as a reference point. Relative location can be expressed as the distance between user *A* and user *B*, user *A* and device *C*, or user *A* and location *D*.

d) ***Categotical Location***: is the location expressed in a predefined category. Some examples include home, office, street, mall, or restaurant.

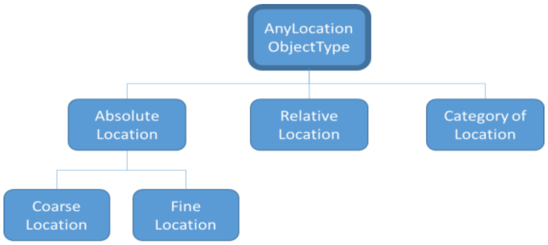


Figure 5. Location Object Types

Referring to Figure 3, a subject has access to an object, only if the access is authorized by the core access control. Also, the subject needs to specify the purposes of the access and the recipients of the result of the access operation. The purposes and the recipients must be legitimated according to the access of the object defined by the owner or an authority such as the government. Thus, obligations and a retention policy will be returned as a response message if the access is allowed. The subject must also comply with the obligations and the retention policies. The access request will be denied otherwise.

Parents can create policy rules for their child's data through the process illustrated in Figure 6. This process is done through a mobile Web interface on the mobile device. The policy rule creation process starts with the initialization phase, whose first step is for the parent to configure themselves as the child (user)'s parent. By mapping a parent to a child user, the parent becomes the owner of the child's data. Next, the parent consents to the End User License Agreement (EULA) on behalf of the child, agreeing to the terms of the mobile service. Lastly, the parent sets their communication channel (e.g., email address) and preferences for receiving acknowledgements of privacy updates related to their child's data. As the second step, the parent can create policy rules according to their preferences for how their child's data can be collected and shared. This model uses positive authorization, in which parents define the rules for what is allowed. To create a policy rule, the parent first specifies the subject (their child), the object (e.g., absolute location data), the allowed operation (e.g., read), the allowed purposes (e.g., game purpose), and the allowed recipients (e.g., other users in-game). Next, the parent specifies the obligations and retention policies that the recipient must comply to in order to receive the data object with an expiry date. After a rule is created, this second step can be repeated to create as many rules as desired. Step 3 shows the administrative tasks to manage the privacy rules.

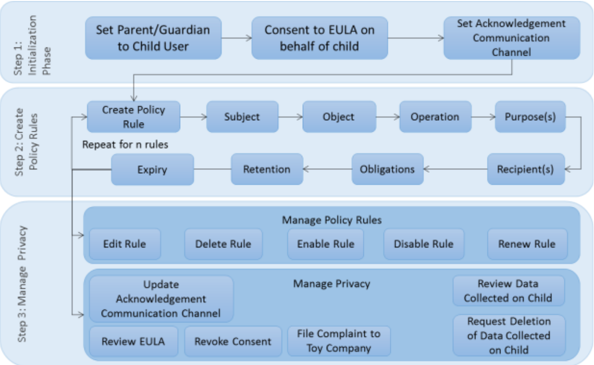

Step 1: Initialization Phase
Set Parent/Guardian to Child User
Consent to EULA on behalf of child
Set Acknowledgement Communication Channel
Step 2: Create Policy Rules
Create Policy Rule
Subject
Object
Operation
Purpose(s)
Repeat for n rules
Expiry
Retention
Obligations
Recipient(s)
Step 3: Manage Privacy
Manage Policy Rules
Edit Rule
Delete Rule
Enable Rule
Disable Rule
Renew Rule
Update Acknowledgement Communication Channel
Manage Privacy
Review Data Collected on Child
Review EULA
Revoke Consent
File Complaint to Toy Company
Request Deletion of Data Collected on Child

Figure 6. Privacy Rule Creation Process

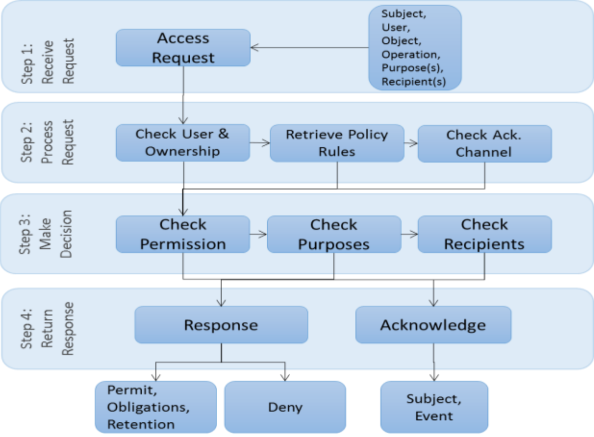


Figure 7. Access Control Decision Process

The access control decision procedure in the privacy access control model is described in Figure 7. A subject first requests access to a user's location information, specifying the subject, object, operation, purposes, and recipients. After receiving the request, as the second step, the privacy access control model processes the request as follows: *(1)* checks the owner of the requested object; *(2)* retrieves the corresponding privacy rules from the system; and, then, *(3)* checks the acknowledgment communication channel for the subject owner. Next, as the third step, the decision is made by: *(1)* checking the permissions from the core access control model; *(2)* checking the allowed purposes; and, then, *(3)* checking allowed recipients.

As the fourth step, the final decision is made and the system returns a response and acknowledgement. The response can be either permit, along with the obligations and retention policy or deny. If applicable, the acknowledgement is sent to the subject owner through the predefined acknowledgement channel, and contains the subject and event. Lastly, the model records all of the above in the audit logs.

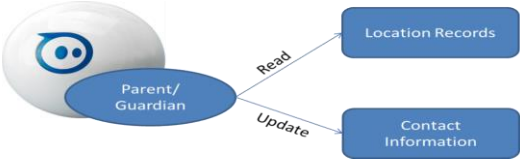


Figure 8. Example Scenario 1: Sphero

4. Discussion

Referring to a toy computing scenario, in this section we present some example scenarios using Tek Recon, and Sphero to illustrate some possible privacy access control rules based on the model.

Scenario 1: Sphero [31] is another recent toy computing product in the industry, first introduced in 2011 by Orbotix, which then released subsequent versions, Sphero 2.0 in 2013 and Sphero Ollie in 2014. Referring to Figure 8, Sphero is a robotic ball which can be controlled and programmed through the user's smartphone or tablet. There are over 30 apps available for Sphero, most of which are games, while others are focused on education. This product is marketed not only to children and can be appropriate for any age group. While the physical ball component is a very simple and traditional concept, the capabilities of the toy increase substantially with the inclusion of robotics and a mobile device. The Sphero ball has wireless networking capabilities, an accelerometer and gyroscope, rolls in every direction, and glows different and a mobile device. The Sphero ball has wireless networking capabilities, an accelerometer and gyroscope, rolls in every direction, and glows different colors. Sphero can be programmed by the user through an app called Sphero Macrolab, which includes a set of predefined macros, and more advanced users can use another app called orbBasic to program in a language based on BASIC. A parent may access their child's location records collected by Sphero. They may update their contact information for receiving acknowledgements. Some examples of privacy rules for this scenario are presented as follows.

Privacy rules:

S1.1: A parent/guardian (data owner) is allowed to read or copy his child's location record

(Parent/Guardian, read, locationRecord, _, _, permit, _, _)
(Parent/Guardian, copy, locationRecord, _, _, permit, _, _)

S1.2: A parent/guardian is allowed to update his/her contact information

(owner, update, ContactInformation, _, _, permit, _, _)

Scenario 2: Tek Recon [32]: is a line of toy blasters developed by Tech4Kids, marketed to children aged 8 years and up in 2013. While this product features a physical component identical in concept to a traditional toy blaster, the novelty is the ability to integrate with a mobile device. Referring to Figure 9, the Tek Recon blaster features a mount on top where a smartphone is inserted. A mobile application has been developed by Tech4Kids which operates in collaboration with the physical blaster to augment traditional blaster-based games. The application provides several functionalities including a scope, which uses the smartphone camera to display what is in front of the user with additional features overlaid on top, such as ammunition, score, radio, and a GPS location map of other players. The application has networking functionality to create and join games with friends over a LAN or mobile network. The user is also required to create an account online, where the scores and account information are stored. As shown in Figure 9, a child using Tek Recon has been connected to a mobile service using location services in a toy computing environment to share his location to their friends and see their locations in return. Once the service receives the user's location record, the service may read and disclose the location information to other players for the purpose of the game, and delete the records immediately after the game is complete. An example of privacy rule for this scenario 2 is presented as follows.

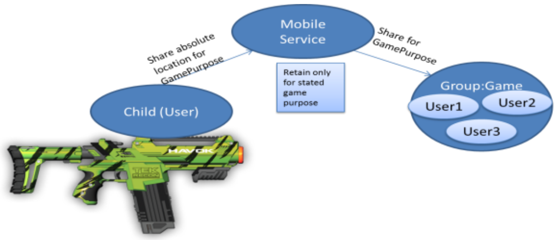


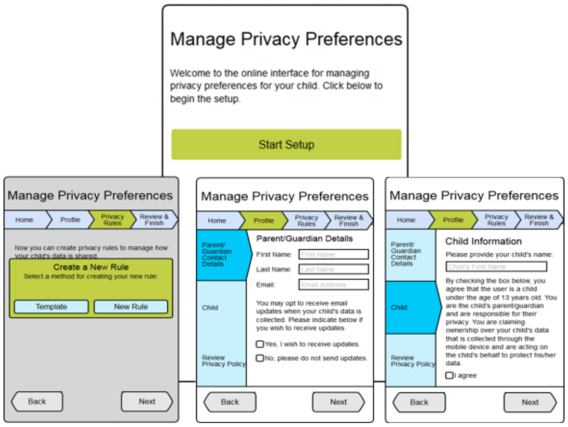
Figure 9. Example Scenario 2: Tek Recon

Privacy rule:

S2.1. A service is allowed to read the absolute location record of a user for the purpose of a game if and only if the service follows obligations of disclosure to group "game" and not to keep the record after stated game purpose has ended.

(MobileService, read, Absolute_Location, GamePurpose, Group:Game, permit, _, StatedPurpose)

Referring to Figure 10, we present a demo of an interface for parents to use in an initial setup to configure preferences and create policy rules. These options would appear during initial setup of a toy computing application. These privacy settings allow parents to create access control rules based on their preferences on concepts from P3P, i.e. purposes, recipients, obligations, and retentions. The first step in the configuration process is the Profile Setup phase. The Profile Setup phase includes three sections, the Parent Contact Details, Child Information, and Privacy Policy Review. The parent enters their basic information including name and email address, and then selects if they wish to receive email updates on their child's privacy-related information. Next, on the Child Information page, the child's first name is entered for management purposes, and the parent then agrees to take ownership over their child's data. Next, the privacy policy of the toy application is presented to the parent to review. The parent reviews the policy and must confirm that they have read and agree to the terms before proceeding. By agreeing to the terms, the parent is providing consent on their child's behalf.



Manage Privacy Preferences

Welcome to the online interface for managing privacy preferences for your child. Click below to begin the setup.

Now you can create privacy rules to manage how your child's data is shared.

Create a New Rule

Select a method for creating your new rule:

Parent/Guardian Details

First Name:

Last Name:

Email:

You may opt to receive email updates when your child's data is collected. Please indicate below if you wish to receive updates.

□ Yes, I wish to receive updates.

□ No, please do not send updates.

Child Information

Please provide your child's name:

By checking the box below, you agree that the user is a child under the age of 13 years old. You are the child's parent/guardian and are responsible for their privacy. You are claiming ownership over your child's data that is collected through the mobile device and are acting on the child's behalf to protect his/her data.

□ I agree

Figure 10. Prototype Interface Demonstration

The next phase is the Privacy Rule creation phase, when the parent is able to create one or more privacy rules for how their child's private location data is used. By default, there is no policy rules yet configured. A new rule can be created or a template can be used. Templates of useful policy rules can be provided to simplify the rule configuration process for parents. The first step of creating a new privacy rule is the General Settings. In the General Settings, the parent can name the rule, provide a description, and set an expiry date for how long the rule will be in effect. Next, in the Core Access Control settings, the mobile service (subject), location resource (object), and operation are selected. The objects selected are the absolute location and relative location. Next, the settings for Purposes and Recipients are also presented. The parent chooses from a list of purposes they wish to accept, as well as a list of types of recipients. The types of recipients can be expanded to be more specific, such as Third-Party: Marketing, or Group: Game Players.

The next steps are the Obligations and Retention settings, and then finally reviewing and adding the rule, as shown in Figure 10, the parent first selects the obligations that the service must comply with upon receiving the child's data. Obligations can include compliance with PIPEDA or COPPA. The parent can also search from a list of other obligations, or input a custom obligation policy. For retention, the parent can select how long they wish to allow their child's data to be retained. Finally, on the Review & Add Rule page, the privacy rule is presented in plain English. Once the parent reviews the rule, they can select "Confirm and Add Rule" at the bottom of the screen. Once a privacy rule is added, the parent is directed to the Manage Privacy Rules page, which shows a table of all of the configured privacy rules and their status (e.g., enabled, disabled, or expired). This provides options to enable, disable, edit, delete, or create new rules. A parent can also return to this screen at a later time to manage rules or renew expired rules. Once the parent is satisfied with the privacy rules, he/she can select "Next" to be directed to the final Review & Finish page. This page summarizes all of the settings and confirms that the parent has completed all of the sections. A list of enabled privacy rules and their corresponding expiry dates is also presented. Finally, the parent can select "Save and Finish" to save their settings and finish the setup. Then the settings will take effect immediately.

5. Conclusions

This paper presented a privacy rule conceptual model for smart toys which is one of the first attempts in this emerging research topic. The model allows parents to create privacy rules and receive acknowledgements regarding their child's privacy sensitive location data. Next, we presented the algorithm for access control decisions for privacy enforcement, and finally we illustrated the applicability of the privacy rules in a practical environment using example scenarios with popular toy computing toys in the industry. We are currently conducting an empirical study to justify the user acceptability of the prototype interface for the privacy rule conceptual model.

6. Acknowledgements

This work was supported by the São Paulo Research Foundation (Fapesp) under Grants 2015/16615-0 and 2016/00014-0. This work was also supported by the Research Office - Zayed University, Abu Dhabi, United Arab Emirates, under Research Projects: R15048 & R16083; by the Ministry of Science and Technology (MOST), Taiwan, under MOST Grants: 105-2923-E-002 -014 -MY3, 105-2923-E-027 -001 -MY3, 105-2221-E-027 -113, & 105-2811-E-027 -001; and the Natural Sciences and Engineering Research Council of Canada (NSERC), under Discovery Grants Program: RGPIN-2016-05023.

7. References

[1] Ren, Y., Shen, J., Wang, J., Han, J., and S. Lee, “Mutual Verifiable Provable Data Auditing in Public Cloud Storage,” Journal of Internet Tech., vol. 16, no. 2, pp. 317-323, 2015

[2] Tath, E. I., “Context Data Model for Privacy,” PRIME Standardization Workshop, IBM Zurich, 6 Pages, 2006

[3] Tanaka, F., and T. Kimura, “The use of Robots in Early Education: A Scenario Based on Ethical Consideration,” the 18th IEEE International Symposium on Robot and Human Interactive Communication, pp. 558 – 560, 2009

[4] Plowman, L., and Luckin, R., “Interactivity, interfaces, and smart toys,” Computer, vol. 37, no. 2, pp. 98 – 100, 2004

[5] Hung, P. C. K., “Mobile Services for Toy Computing,” the Springer International Series on Applications and Trends in Computer Science, Springer International Publishing, 2015

[6] Schell, B. H., Martin, M. V., Hung, P. C. K., and L. Rueda, “Cyber Child Pornography: A Review Paper of the Social and Legal Issues and Remedies, Aggression and Violent Behavior,” Elsevier, vol. 12, no. 1, pp. 45 – 63, 2007

[7] Xia, Z., Wang, X., Sun, X., and Q. Wang, “A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data,” IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 340-352, 2015

[8] AlHarthy, K., and W. Shawkat, “Implement network security control solutions in BYOD environment,” the 2013 IEEE International Conference on Control System, Computing and Engineering (ICCSCE), pp. 7 – 11, 2013

[9] Armando, A., Costa, G., Verderame, L., and A. Merlo, “Securing the Bring Your Own Device Paradigm,” Computer, Volume: 47, Issue: 6, pp. 48 – 56, 2014

[10] Peng, W., Li, F., Han, K.J., Zou, X. K., and J. Wu, “T-dominance: Prioritized defense deployment for BYOD security,” the 2013 IEEE Conference on Communications and Network Security (CNS), pp. 37 – 45, 2013

[11] Alqassem, I., and D. Svetinovic, “A taxonomy of security and privacy requirements for the Internet of Things (IoT),” the IEEE International Conference on Industrial Eng. and Engineering Management, pp. 1244 – 1248, 2014

[12] Sun, G., Huang, S., Bao, W., Yang, Y., and Z. Wang, “A Privacy Protection Policy Combined with Privacy Homomorphism in the Internet of Things,” the 23rd International Conference on Computer Communication and Networks (ICCCN), pp. 1 – 6, 2014

[13] Cherubini, M., de Oliveira, R., Hiltunen, A., and N. Oliver, “Barriers and bridges in the adoption of today's mobile phone contextual services,” in MobileHCI '11, Sweden, 2011

[14] MEF, “MEF Global Privacy Report 2013,” MEF, 2013

[15] Futuresight, “User Perspectives on Mobile Privacy - Summary of Research Findings,” GSMA, 2011

[16] Chakraborty, S., Raghavan, K. R., Johnson, M. P., and M. B. Srivastava, “A Framework for Context-Aware Privacy of Sensor Data on Mobile Systems,” in The Fourteenth Workshop on Mobile Computing Systems and Applications (ACM HotMobile2013), New York, USA, 2013

[17] Heurix, J., Zimmermann, P., Neubauer, T., and S. Fenz, “A taxonomy for privacy enhancing technologies,” Computers and Security, 53, pp. 1 – 17, 2015

[18] Atamli, A., and A. Martin, “Threat-Based Security Analysis for the Internet of Things,” the 2014 International Workshop on Secure Internet of Things, pp. 35 – 43, 2014

[19] Barnes, R., Lepinski, M., Cooper, A., Morris, J., Tschofenig, H., and H. Schulzrinne, “An Architecture for Location and Location Privacy in Internet Applications,” Internet Engineering Task Force (IETF), 2011

[20] Duri, S., Cole, A., Munson, J., and J. Christensen, “An approach to providing a seamless end-user experience for location-aware applications,” the 1st International Workshop on Mobile Commerce, vol. 86, no. 4, 20 Pages, 2001

[21] Pura, M., “Linking perceived value and loyalty in location-based mobile services,” Managing Services Quality, vol. 15, no. 6, pp. 509-538, 2005

[22] Baber, C., and O. Westmancott, “Social networks and mobile games: the use of bluetooth for a multiplayer card game,” the 6th International Conference on Human Computer Interaction with Mobile Devices and Services, Glasgow, Scotland, 2004

[23] Rovio, “Angry Birds,” 2015. [Online]. Available: http://www.rovio.com/en/our-work/games/view/1/angry-birds

[24] Booyah, “iTunes - MyTown2,” 2015. [Online]. Available: https://itunes.apple.com/app/mytown-2/id442345455

[25] Kaasinen, E., “User Needs for Location-Aware Mobile Services,” Personal and Ubiquitous Computing, vol. 7, no. 1, pp. 70-79, May 2003

[26] Wenning, R., “Platform for Privacy Preferences (P3P) Project: Enabling Smarter Privacy Tools for the Web,” 20 November 2007. [Online]. Available: http://www.w3.org/P3P/

[27] Shen, J., Moh, S., and I. Chung, “Enhanced Secure Sensor Association and Key Management in Wireless Body Area Networks,” Journal of Communications and Networks, vol. 17, no. 5, pp. 453-462, 2015

[28] Fu, Z., Ren, K., Shu, J., Sun, X., and F. Huang, “Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement,” IEEE Transactions on Parallel and Distributed Systems, 2015

[29] He, Q., “Privacy enforcement with an extended role-based access control model,” NCSU Computer Science Technical Report TR-2003-09, February 2003

[30] Android, “Location Strategies,” Android Developer, 2015. [Online]. Available: http://developer.android.com/guide/topics/location/strategies.html

[31] Sphero, “Sphero,” 2014. [Online]. Available: http://www.gosphero.com

[32] Tech4Kids, “Tek Recon,” Tech4Kids, 2013. [Online]. Available: http://www.tekrecon.com/

[33] Niantic, Inc., “Pokemon Go,” 2016. [Online]. Available: http://www.pokemongo.com/