Proceedings of the Future Technologies Conference (FTC) 2018

Author(s) Arai, Kohei; Bhatia, Rahul; Kapoor, Supriya

Imprint Springer International Publishing, 2019

ISBN 9783030026868, 9783030026851

Permalink https://books.scholarsportal.info/uri/ebooks/ebooks4/springer4/2019-07-01/1/9783030026868

Pages 152 to 158

Toys That Talk to Strangers: A Look at the Privacy Policies of Connected Toys

Wahida Chowdhury(✉)

University of Ottawa, Ottawa, ON, Canada
Wahida.Chowdhury@hotmail.ca

Abstract. Toys that are connected to the Internet are able to record data from users and share the data with company databases. The security and privacy of user data thus depend on companies' privacy policies. Though there is a rising concern about the privacy of children and parents who use these connected toys, there is a scarcity of research on how toy companies are responding to the concern. We analyzed privacy policies of 15 toy companies to investigate the ways toy companies publicly document digital standards of their connected products. Our results show that most toy companies are either unclear or do not mention in their privacy policy documents how their toys protect the security and privacy of users. We recommend measures that toy companies may adopt to explicitly respond to security and privacy concerns so parents can make informed decisions before purchasing the connected toys for their children.

Keywords: Connected toys · Smart toys · Internet of Things
Information privacy · Data security · Privacy policies · Digital standards
Children · Parents

1 Introduction

Toys that gather information from owners via microphone, camera or user inputs, and share the information via Internet to whomever these toys are connected to, are known as connected toys. These toys may replace traditional friends by being highly interactive such as by recording the child's preferences and by talking back to the child. These toys may also replace traditional baby sitters and keep the child busy when parents are working. Toy companies quickly noted these benefits and advertised their connected products to children and parents by obscuring associated risks to privacy and data security. For example, Edwin the Duck uses Bluetooth technology to broadcast lullabies to its young users; however, the toy company also collects and retains everything the child says and shares that information with "trusted" third parties. The purpose of our research was to investigate the extent to which connected toy companies respond to benefits versus threats towards consumers' privacy and data security.

We analyzed the privacy policies of 15 connected toys; the connected products were selected from the privacy guide developed by Mozilla foundation, a not-for-profit organization that supports and promotes the use of connected products. We asked 16 questions about the privacy and data security of each product and looked through the

K. Arai et al. (Eds.): FTC 2018, AISC 880, pp. 152–158, 2019.
https://doi.org/10.1007/978-3-030-02686-8_12

manufacturers' privacy policies for answers. The results provide a snapshot of the informational practices of the connected toy companies, and recommend ways to make privacy policies more explicit so consumers can make informed decisions before purchasing.

2 Literature Review

Connected toys relate to 'a future in which digital and physical entities can be linked, by means of appropriate information and communication technologies, to enable a whole new class of applications and services' [1]. A wide variety of toys fall under the domain of connected toys. Some of these toys are connected to voice and/or image recognition software (e.g. Hello Barbie™ or the Hatchimals); some are connected to app-enabled robots, and other mechanical toys (e.g. Dash and Dot); and others are connected to video games (e.g. Skylanders or Lego Dimensions) [2]. Some connected toys are connected to the Internet but do not simulate human-like behaviour; some toys simulate human interaction by talking to users; and other toys such as connected robots can be coded by users to perform novel activities [3].

Mascheroni & Holloway (Eds.) (2017) Identified articles about connected toys from 12 countries (Australia, Austria, Finland, Germany, Italy, Lithuania, Malta, Portugal, Romania, Serbia, Slovenia and Spain), and documented the benefits of connected toys as reported by parents. The benefits included the development of digital literacy, creativity, motivation to learn, reading and writing literacy, social skills, physical activity, etc. Despite the benefits however, concerns about the security and privacy of users (who are primarily children) are documented in the literature from the hay days of connected toys [4].

Concerns about children's security and privacy were already in place as social networking, gaming, and other websites gathered, stored, and shared data from child users with other third parties often without the child users' knowledge or consent [5]. Connected toys intensified the concerns by making data collection from children easier (such as by microphone, camera, location tracker, and movement detectors) and by being able to collect more personal data (such as by being able to follow child users everywhere and by being always "on"). The developments exacerbated the risks of easy access to personal information, simply by hacking company databases. Recent examples include hacking of data collected by the connected toys, Hello Barbie and VTech, from millions of child users [2].

The security and privacy concerns imply that toy makers should incorporate effective measures from inception to completion of the development process of connected toys [6]. Our research looks into the privacy policies of toy companies to report how the companies are addressing public hopes and fears surrounding connected toys.

3 Methodology

The Mozilla foundation published a report, *Privacy Not Included,* in December 2017 that reviewed openly accessible privacy policies of different connected products. The

report aimed to draw buyers' attention to three questions related to privacy and security before purchasing the products: (1) How do the products spy on users? (2) What information about the users do the products collect? and (3) What could happen to users if data breeches occur? For example, Mozilla guide reports that the connected toy, Dash the Robot, is a one-eyed robot that can sing, dance, and play to give an highly interactive and fun experience to children; however, parents should be warned that the robot can spy on children via microphone and that parents have no control over the data that the robot collects.

To extend the Mozilla product reviews and have more in-depth synopsis of users' privacy and data security related to connected products, we conducted further analyses of the privacy policies of 15 toys and game consoles listed in the Mozilla report. These connected products were: Smart letters, Edwin the Duck, Adidas miCoach Smart Soccer Ball, Ozobot Evo, Beasts of Balance, Toymail Talkie, Sphero SPRK+, Osmo, Dash the robot, BB-8 by Sphero, Airjamz Air Guitar, Hello Barbie, Microsoft Xbox One, Sony Playstation 4, and Nintendo Switch.

We developed 16 distinct questions from the open access Digital Standards, created by Consumer Reports, Disconnect, Ranking Rights and the Cyber Independent Testing Lab to evaluate the privacy and security of the 15 connected toys. For example, we investigated how secure user information is when using a connected product; we looked through the product's privacy policies to determine if the company routinely audits user data and restricts third party access to the data. The various questions answered what privacy measures were put in place, what privacy controls were available, and what kind of information the companies gathered from users and disclosed to third parties.

4 Results

4.1 How secure is users' data?

Almost all the companies we studied claimed that they take steps or comply with standards to protect user data, but they are not always clear about what steps they take or what standards they follow. Furthermore, none of the companies we studied are confident that they are hack-proof, and admit that security breaches can still happen.

4.2 Do users need to make a password?

Most companies require users to make a password. However, passwords are not required to be complex/secure. This means that the user information could be easily hacked.

4.3 Does the company encrypt users' information?

Only four (27%) of the companies we studied fully encrypt user data; others partly encrypt users data or do not encrypt at all. This means that the user information could be easily understood if hacked.

4.4 Can users control the data that the company collects?

Almost half the companies we studied (53%) do not mention if users can control their own data. In fact, few companies such as "osmo" toy automatically collect information without user control.

4.5 Can users delete their data when they leave the service?

Almost all the companies we studied allow users to delete data when they leave services, but maybe not completely. For example, companies may retain non-personally identifiable data, and catched or backup copies of user data that companies are not explicit about. This means that even if users leave a service, their information could be hacked.

4.6 Do users know what information the company collects?

Almost all the companies we studied give users snapshots of what information is collected from them. However, the hidden rules are often too complex to understand and are easy to overlook.

4.7 Does the company collect only the information needed for the product to function?

Almost all the companies we studied collect more information from users than what is needed to make their product work.

4.8 Is users' privacy protected from third parties by default?

None of the companies we studied protect user data from third companies by default. Some companies allow users to review and change their privacy settings. However, it is not clear to what extent users are able to protect their privacy without loosing access to services.

4.9 How does the company use users' data?

The privacy documents of almost all the companies we studied explicitly state how they might use user data. However, most companies leave the responsibility on users to control their own privacy, and users are threatened that they might not get the best service if they restrict access to their data.

4.10 Does the company have a privacy policy document?

All the companies we studied have privacy policy documents. However, the documents are often very long in a tangible language, and often so not answer important questions.

4.11 Will users receive a notification if the company changes its privacy policy?

Less than half (40%) of the companies we studied send notifications if their privacy policies change. Most companies either do not mention of any change or simply update the date on top of their policy documents that are very unlikely to be read twice by users to notice the change.

4.12 Does the company comply only with legal and ethical third-party requests for users' information?

Only 27% of the companies we studied explicitly mentioned that they comply only with legal and ethical third-party requests of user information. Most companies claim to share non-identifiable information or are not explicit about how information requests are handled.

4.13 Does the company require users to verify identity with government-issued identification, or with other forms of identification that could be connected to users' offline identity?

None of the companies we studied require users to verify identity with government-issued identification, indicating that users can register for services under false names.

4.14 Does the company notify users for any unauthorized access to data?

Only two (13%) of the companies we studied notified users of security breaches. This means that users may continue to use connected products even after these are hacked.

4.15 Is the company transparent about its practices for sharing users' data with the government and third parties?

Only four (27%) of the companies we studied were transparent about sharing practices with the government and third parties.

4.16 Does the company send notifications if the government or third parties request access to users' data?

Only three (2%) of the companies we studied notified users of third party requests. This means that third parties may collect users' information without their awareness.

5 Discussion

Childhood experiences are rapidly becoming digital by including connected toys and games that let children connect to strangers effortlessly from the comfort of their home. Although this may seem fun and safe, our findings indicate that none of the toys provided

satisfactory answers to all 16 questions related to privacy and data security. There remained a variety of different ways a connected toy company may gather information, such as recording users preferences, tracking a user's IP address and turning on a device's camera every time the toy is used. The security of user information thus relies on the security of the databases of a connected toy company or of the third parties that the company shares information with. If hackers or even employees access the databases with any wrong motive from having fun to stealing money to initiating a cyber-war, strangers can talk back to the young users and make them do inappropriate things.

To prevent data breeches, privacy policy documents of the 15 toy companies that we analyzed claimed to have privacy measures in place; this might make parents feel relieved to trust the companies to be responsible care takers of their children. However, the privacy policies of almost all the companies accepted that their databases might not be secure enough to prevent data breeches. Companies seem to posit that users are responsible for their own security. However, users were often threatened of losing services if they exercised control of their privacy, for example if users did not share data with third parties.

The privacy policies of each company attempt to document their data collection and sharing practices that might give the feeling of making an informed decision about purchasing the company products. However, the policies do not follow a standardized format and are not always written in a way that the general user could understand. Also the definitions of privacy measures such as data control and data collection are not standardized between companies. This means that many parents may not be aware of the information that companies gather about their children which may limit their ability to make fully informed decisions about the products that they're purchasing. For example, when a parent signs up for an account for various toys or consoles, certain information is asked of them but the sign up mechanisms do not draw the parent's attention to the fact that the toy's microphone may be accessed or that the child's IP address and/or Wi-Fi information may be stored in the company servers.

Furthermore, users may ignore reading lengthy documents, such as ambiguous privacy policies, that describe before purchasing what a certain connected toy does. For example, users may ignore ambiguous warning that a toy maybe harmful which does not state clearly why or how the toy may be harmful. Users may also feel if a product is in the market, the company must have done security checks. For example, if a new car is in the market, users should not have to think if the car would be safe for driving; let alone, investigating if children's toys are safe for playing.

6 Recommendations for Toy Companies

Our findings suggest that a Frequently Asked Questions or FAQ should accompany privacy policy documents that itemize privacy-related questions the way we did in this report so it's easier for people to see how their information is collected, used and disclosed. Secondly, if the concerns stem from sharing data with company databases, toy companies should re-consider the necessities of sharing data with remote databases

that have the possibility of being hacked, rather than sharing data locally within the toy itself that can only be hacked if the child loses the toy.

Furthermore, more evaluations need to be done, as new toys are developed to ensure that children's information is given the highest level of protection. Manufacturers should strive to make connected toys more reliable and capable each year while service providers, software engineers, governments, private organizations, and technical experts should strive to prevent and solve security and socio-economic problems arising from connected toys.

Acknowledgment. The author wishes to thank Diana Cave (Criminology Department, University of Ottawa) for assisting in conducting the research, and professor Valerie Steeves (Criminology Department, University of Ottawa) for her valuable comments on previous drafts of this article.

References

1. Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I.: Internet of Things: vision, applications and research challenges. Ad Hoc Netw. **10**(7), 1497–1516 (2012). https://doi.org/10.1016/j.adhoc.2012.02.016
2. Holloway, D., Green, L.: The internet of toys. Commun. Res. Pract. **2**(4), 506–519 (2016)
3. Mascheroni, G., Holloway, D. (eds.): The Internet of Toys: A Report on Media and Social Discourses Around Young Children and IoToys. DigiLitEY, London (2017)
4. Dobbins, D.L.: Analysis of security concerns and privacy risks of children's smart toys. Ph.D. Dissertation. Washington University St. Louis, St. Louis, MO, USA (2015)
5. Steeves, V., Jones, O.: Surveillance, children and childhood (Editorial). Surveill. Soc. **7**(3/4), 187–191 (2010)
6. Nelson, B.: Children's Connected Toys: Data Security and Privacy Concerns. United States Congress Senate Committee on Commerce, Science, and Transportation, 14 December 2016. https://www.hsdl.org/?view&did=797394. Accessed 4 July 2017