Safe Toys: An Analysis of Various Privacy Policies of Toys and Game Consoles

By: Diana Cave Supervised by: Valerie Steeves, Department of Criminology

Introduction

Mozilla published a report in December 2017 that itemized how toys that connect to the Internet can be used to "spy" on the children who play with them. For example, Edwin the Duck uses Bluetooth technology to enable the company to talk directly to its young users; however, the company also collects and retains everything the child says and shared that information with "trusted" third parties. To get a better understanding of how this occurs, we conducted a series of privacy analyses on 15 toys and games listed in the report. The results provide a snapshot of the informational practices of the connected toy industry.

Methodology

Fifteen toys were chosen from the Mozilla report, *Privacy Not Included*, and were analyzed using 16 distinct open-access tests created by Consumer Reports, Disconnect, Ranking Rights and the Cyber Independent Testing Lab. For example, we looked at: data control; security of user data; and data collection. The various tests identified what privacy measures were put in place, what technical controls were available, and whether or not companies disclosed the information they gather to third parties.

General Conclusions

Our findings indicate that all 15 toys collect information in some manner. There were a variety of different ways a company can gather information, such as tracking a user's IP address and turning on a device's camera when the toy was in use. All 15 toys also had some privacy measures in place. However, none of the toys satisfied all 16 tests. In addition, the privacy policies were not always written in a way that the general user could understand, and the definitions of privacy measures such as data control and data collection were 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 wifi information may be stored in the company servers.

References and Acknowledgements

I'd like to thank Dr. Valerie Steeves for giving me the opportunity for being her UROP student and to participate in this research.

I'd also like to thank Dr. Wahida Chowdhury for assisting me with gathering the data for this research.

Thanks to Mozilla Foundation for publishing the initial report; and to Consumer Reports, Disconnect, Ranking Rights and the Cyber Independent Testing Lab for making the tests available to researchers.

13%

- Only two (13%) of the companies we studied notified users of security breaches.
- This means that there can be unauthorized access to users information and they may be unaware of the security breach.

53%

- Only half (53%) of the toys we analyzed mention that users have some control over the information collected from them.
- This means that the other half have no mention in their privacy policy if users have any control over the information collected from them.

0%

- None of the companies that were analyzed protect users' information from 3rd parties by default.
- This means that every company can share information with 3rd party corporations in some way.

Next steps…

Our findings suggest that there needs to be a generalized format for privacy policies so it's easier for people to see how their information is collected, used and disclosed.

General users need to have access to the information that is gathered from them and have more of a say with what is or isn't kept within the company records.

More evaluations need to be done as new toys are developed to ensure that children's information is given the highest level of protection.