Catholic University Journal of Law and Technology

Volume 25 | Issue 2 Article 4

2017

Protecting Privacy in the Era of Smart Toys: Does Hello Barbie Have a Duty to Report

Corinne Moini
University of Richmond School of Law

PROTECTING PRIVACY IN THE ERA OF SMART TOYS: DOES HELLO BARBIE HAVE A DUTY TO REPORT?

Corinne Moini

INTRODUCTION TO HELLO BARBIE

"'Yay, you're here!' Barbie said eagerly. 'This is so exciting. What's your name?'…'I just know we're going to be great friends.'"[1] With a simple greeting, Hello Barbie has infiltrated your child's life. Each time your child wishes to engage, they simply press on Barbie's belt buckle and speak. Unlike other talking toys, the button on Barbie's belt is not to play one of the pre-recorded statements that are installed in the toy.[2] Instead, the button is used to record and transmit what your child says to an online storage cloud where it will be reviewed and used to create an appropriate response. As a playmate, Hello Barbie utilizes Internet connectivity and other advanced technologies including speech recognition to deliver a truly interactive, responsive experience for your child.

Despite Hello Barbie's simplistic and petite appearance,[3] the interior of the doll contains an intricate and advanced hardware system including an integrated circuit board with a "Wi-Fi module, flash memory, audio codec,"[4] and a processing unit. These features allow Barbie to engage in a two-way conversation, play games, and even tell jokes.[5] To make this possible, Mattel collaborated with ToyTalk, the entertainment and technology company that developed

1 James Vlahos, *Artificially Yours*, N.Y. TIMES, Sept. 20, 2015, at MM44.

2 *Id.*

3 "…your child will not notice any difference. Hello Barbie remains as an 11.5 inch fashion doll." MATTEL, HELLO BARBIE MESSAGING/Q&A 3 (2015), http://hellobarbiefaq.mattel.com/wp-content/uploads/2015/12/hellobarbie-faq-v3.pdf [hereinafter HELLO BARBIE FAQS].

4 *Hello Barbie Security: Part 1—Teardown*, SOMERSET RECON (Nov. 20, 2015), http://www.somersetrecon.com/blog/2015/11/20/hello-barbie-security-part-1-teardown.

5 HELLO BARBIE FAQS, *supra* note 3, at 1.

the speech recognition and progressive learning technologies for Hello Barbie.[6] ToyTalk is the brains behind the operation, providing Hello Barbie with a database of 8,000 lines of dialogue and maintaining the secured cloud-based data servers, which helps Barbie "remember" previous conversations with a child.[7] ToyTalk remains heavily involved with Hello Barbie after she has entered into your child's life. The company monitors the conversations between Barbie and your child to make Barbie more realistic and ultimately your child's best friend. In efforts to create a popular and realistic doll, ToyTalk and Mattel conducted several testruns with a child participant and Hello Barbie.[8] Consider the following interaction from one of these test runs:

"'Hey, new question,' Barbie said. Do you have any sisters?' 'Yeah,' Tiara said. 'I only have one.' 'What's something nice that your sister does for you?' Barbie asked. 'She does nothing nice to me,' Tiara said tensely. Barbie forged ahead. 'Well, what is the last nice thing your sister did?' 'She helped me with my project- and then she destroyed it.'" "'No. She is not cool,' Tiara said, gritting her teeth."[9]

If Hello Barbie can get Tiara to divulge this much information during a test run, imagine how much more a child will tell Barbie once the child feels comfortable with her. This recorded conversation between Barbie and Tiara may seem trivial but consider a different situation.

What if Tiara gets to take Barbie home with her that day and she continues to play with Barbie. Barbie soon becomes one of her favorite toys and Tiara tells Barbie everything. "Everything" includes the sexual abuse and molestation that goes on at her aunt's home. In fact, Tiara confides in Barbie frequently, making statements like "Barbie, I don't like to go to there," or "I don't like to be touched by my uncle." Instantly, this recorded speech about Tiara's sexual molestation becomes important and potentially vital for Tiara's health and safety.

To this point, ToyTalk has created automatic responses for serious conversations including bullying, religion, and making friends. Such responses include "[t]hat sounds like something you should talk to a grown-up about" or "[there] is nothing to feel bad about."[10] It remains unclear however, if ToyTalk has created a response plan to deal with statements of abuse and neglect. Based on the Hello Barbie FAQs and test run conversations, Barbie will respond with "[t]hat

---

6 *See id.* at 2.

7 *See id.* at 3.

8 *See* Vlahos, *supra* note 1.

9 *Id.*

10 *See id.*

sounds like something you should talk to a grown-up about"[11] and redirect the conversation.[12] But is this enough? What if Tiara never tells her parents and Tiara continues to be molested? What if the grown-up is the person responsible for molesting Tiara? This means Tiara's recorded speech will likely go unreported and become one of the many soundbites stored in ToyTalk's databases.

This article considers scenarios like the one described above. Existing privacy laws and common law tort duties fall short of providing protection for such instances. The Children's Online Privacy Protection Act ("COPPA") is an effective piece of legislation that protects the privacy rights of minors under the age of thirteen. It requires companies to obtain parental consent and disclose what information is being collected about a minor,[13] but it does not impose any reporting requirements regarding suspected child abuse and neglect. State common law duties to report, on the other hand, do require persons to report known or suspected child abuse and neglect;[14] however the "persons" required to report are limited and vary from state to state. The absence of mandatory reporting in COPPA and the selective reporting requirements in state statutes create a gap. This "gap" is the focus of this article. More specifically, this article proposes that a duty to report recorded speech about abuse and neglect must be added to COPPA to bridge the gap. These instances may not occur frequently, but when companies like ToyTalk are already reviewing and sorting through recorded speech, such a duty should exist.

There are several other implications of Hello Barbie that go beyond the scope of this article. In fact, there are inherent privacy, constitutional, and ownership concerns that emerge with this "intelligent" doll. Privacy issues, not including the issues discussed below, arise from ToyTalk's use of a storage cloud.[15] Recent data hacks have raised concerns regarding the security of these online storage clouds, as well as questions of who has access to this data.[16] Ad-

---

11 *Id*. "The doll's conversation tree has been designed to re-direct inappropriate conversations. For example, Hello Barbie will not repeat curse words. Instead, she will respond by asking a new question." HELLO BARBIE FAQS, *supra* note 3, at 3.

12 *See* HELLO BARBIE FAQS, *supra* note 3, at 3.

13 *See* Children's Online Privacy Protection Rule, 16 C.F.R. § 312.1 (2001).

14 ADMINISTRATION FOR CHILDREN AND FAMILIES: CHILDREN'S BUREAU, MANDATORY REPORTERS OF CHILD ABUSE AND NEGLECT 1 (2015), *available at* https://www.childwelfare.gov/pubPDFs/manda.pdf [hereinafter MANDATORY REPORTERS OF CHILD ABUSE AND NEGLECT].

15 *See, e.g.*, SOMERSET RECON, INC., HELLO BARBIE INITIAL SECURITY ANALYSIS (2016), *available at* https://static1.squarespace.com/static/543effd8e4b095fba39dfe59/t/56a66d424bf1187ad34383b2/1453747529070/HelloBarbieSecurityAnalysis.pdf.

16 Earlier this year, a security researcher hacked The Hello Barbie storage cloud rather easily. He demonstrated that several unwanted parties can have access to a child's information. Thus, the threat of a true security breach, like the one that occurred with VTech this

ditionally, the toy makers of a similar interactive doll, My Friend Cayla, are the subject of a FTC deceptive marketing and violation of collection of personal data of children lawsuit.[17]

A second issue that emerges with Hello Barbie relates to the Fourth Amendment. Specifically, if there is legal action that somehow relates to this doll, the recorded conversations will more than likely be used for litigation purposes.[18] Finally, there is an issue of ownership of recorded speech and First Amendment rights. This issue, like the constitutional issue briefly described above, is present with other types of weak artificial intelligence[19] such as Siri.[20] The remainder of this article will focus solely on the privacy issues relating to data collection of a minor's speech. More specifically, this article will focus on who has access to the conversations between a child and Hello Barbie that are stored on the cloud, and what their duty must be if presented with a situation like Tiara's above.

The article proceeds as follows: Part II addresses the current state of technology and data collection. This Part also introduces the legal implications of data collection and the common-law duty to report. Part III provides a detailed background of the relevant privacy laws that govern artificial intelligence and data collection companies. Part III also provides a more in-depth discussion of the "gap" identified above. Part IV provides a possible solution to bridge this

---

year, is present and possible. *See* Sarah Griffiths, *The Dark Side of Buying Your Children Smart Toys: Expert Warns Hello Barbie can be Hacked, as VTech Suffers Major Data Breach*, DAILY MAIL (Dec. 2, 2015), http://www.dailymail.co.uk/sciencetech/article-3340789/The-dark-buying-children-smart-toys-Expert-warns-Hello-Barbie-hacked-VTech-suffers-major-data-breach.html.

17 "In December 2016, five advocacy groups filed a complaint with the FTC about the data collection practices of the My Friend Cayla doll. The doll is very similar to Hello Barbie recording a child's speech and using speech recognition technology to craft an appropriate response. My Friend Cayla uses Blue-Tooth technology instead of Wi-Fi." Jeff John Roberts, *Privacy Groups Claim These Popular Dolls Spy on Kids*, FORTUNE (Dec. 8, 2016), http://fortune.com/2016/12/08/my-friend-cayla-doll/. *See* Complaint and Request for Investigation, Injunction, and other Relief at 2, *In re* Genesis Toys & Nuance Communications, (FTC Dec. 6, 2016), *available at* https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf.

18 This is because Hello Barbie will likely not be included in the umbrella clause "in their persons, houses papers, and effects" of the Fourth Amendment, based on previous use of GPS location data in litigation. *See* U.S. CONST. amend. IV; *see* Frank Lin, *Siri, Can You Keep a Secret? A Balanced Approach to Fourth Amendment Principles and Location Data*, 92 OR. L. REV. 193, 196 (2013).

19 *See infra* Section II.

20 Who owns any potential intellectual property that arises from the interaction between child and Barbie? This is unclear for numerous reasons ranging from the child's minor status to the fact that Siri and Barbie are not natural persons.

gap. More specifically, it suggests a potential amendment to COPPA. This article will discuss the pros and cons of such an amendment and close with a brief conclusion.

THE CURRENT STATE OF DATA TECHNOLOGY

In today's society, technology is commonplace. School-age children have access to laptop computers, smart screens, and smart phones as early as kindergarten.[21] Young adolescents are among the fastest growing segment of the population that uses popular social media apps such as Snapchat and Instagram.[22] We are witnessing a deep transformation in the way an entire generation utilizes technology as its primary means to interact and communicate with peers. Children are by far more receptive to adopting and using new technologies than previous generations and express little or no concern about the privacy implications associated with using these technologies and devices.[23] They seem to be open to trading their privacy in return for gaining access to social media and other online services.[24] Companies are taking advantage of this by directly marketing and targeting children from a young age.[25] The advertisements suggest that there are safeguards for young children accessing smart toys or applications, such as "safe-Wi-Fi" and age requirements.[26] For example, VTech, an electronic learning product company, sells tablets for children as

---

21 *See* David Nagel, *One-Third of U.S. Students Use School-Issued Mobile Devices*, THE JOURNAL (Apr. 8, 2014), https://thejournal.com/articles/2014/04/08/a-third-of-secondary-students-use-school-issued-mobile-devices.aspx ("Half of students in grades 3–5 have access to a smart phone, though only 21 percent of K–2 students can make that claim. Laptops and tablets are even more entrenched. Sixty-two percent in grades 3–5 have access to laptops, and 58 percent have access to tablets. In grades K–2, 41 percent have access to laptops and/or tablets. Thirty-nine percent in grades 3–5 have access to digital readers, 18 percent in grades K–2.").

22 Adam McLane, *Which Social Media Apps are Middle Schoolers Using Right Now?* ADAM MCLANE (Oct. 15, 2013), https://adammclane.com/2013/10/social-media-apps-middle-schoolers-using-right-now/.

23 *See* Chris Nickson, *How a Young Generation Accepts Technology*, A TECH. SOC. (Nov. 29, 2016), http://www.atechnologysociety.co.uk/how-young-generation-accepts-technology.html.

24 *Id.*

25 Studies suggest that marketing to children is like marketing to three different markets at once: the child itself, the future market for goods and services, and the parents. *See* James U. McNeal, *From Savers to Spenders: How Children Became a Consumer Market*, CTR. FOR MEDIA LITERACY, http://www.medialit.org/reading-room/savers-spenders-how-children-became-consumer-market (last visited Mar. 30, 2017).

26 *See, e.g.*, *InnoTab 3 Plus*, VTECH, https://www.vtechkids.com/brands/brand_view/innotab3splus (last visited Nov. 30, 2016) (discussing the kid-safe Wi-Fi options with the InnoTab 3 Plus).

young as three years old.[27] According to its website, certain tablets such as the InnoTab 3S Plus, provide "kid-safe Wi-Fi,"[28] which simply means that it pre-selects appropriate websites for children ("VTech Selected Sites") and gives parents the ability to further control their child's access.[29] However, are the safeguards enough? This section will provide a brief discussion of the specific technology behind Hello Barbie, followed by a general discussion of artificial intelligence and data collection. This section will also provide initial insights to what these technologies take from their consumers.

A. Technology Behind Hello Barbie

Like many inventions, the idea for Hello Barbie came from a rather unexpected source —a child. About five years ago, a young girl named Toby asked her father, Oren Jacob, the former Chief Technology Officer at Pixar, if she could talk to "her favorite stuffed animal, a fuzzy rabbit she called Tutu" on an iPhone.[30] At first Jacob "says he just laughed at his daughter's remark" but it later sparked the idea for his new company ToyTalk.[31] Since 2011, Jacob and his business partner Martin Reddy have been working on creating products such as "smartphone and tablet apps featuring characters that talk back."[32] In 2015, ToyTalk began working with Mattel to create Hello Barbie.[33] Together, Mattel and ToyTalk have taken traditional play and make-believe to an unprecedented space.

Prior to Hello Barbie, companies like Mattel and Hasbro created semi-interactive toys, capable of playing back a fixed number of prerecorded messages.[34] Such recorded statements include "Want to have a pizza party?" or

---

27 *See InnoTab 3Plus - The Learning Tablet*, VTECH, https://www.vtechkids.com/product/detail/15811/InnoTab_3_Plus___The_Learning_Tablet (last visited Dec. 1, 2016).

28 *InnoTab 3S User's Manual*, VTECH (2014), https://www.vtechkids.com/assets/data/products/%7BBEBD32C2-32CC-4F78-AFCB-CD0C68EB886A%7D/manuals/158808InnoTab3SPlusProductManual_051314(2014)_FINAL.pdf.

29 *See id.* Parents can modify VTech Selected Sites and add and limit other websites. It also states "VTech® is not responsible for any inappropriate content that might be found on the Web. Parents should use caution when allowing their children to go online and should continue to monitor the online activities of their children closely." *Id.*

30 Vlahos, s*upra* note 1.

31 *Id*.

32 *Id.*

33 *See id.* ToyTalk's projected sales for Hello Barbie equals about 6 billion dollars.

34 *Id*. Throughout history, innovation has driven the development of talking toys. Examples include "inventors in the mid1800s[] deploying bellows in place of human lungs and

"Math is hard!"[35] These toys are not able to participate in a true conversation with a child, because they lack true speech generation and are limited to the "hidden record players, cassette tapes or digital tips" integrated into the toy.[36] In 2014, Genesis Toys released My Friend Cayla doll.[37] Similar to Hello Barbie, My Friend Cayla uses Bluetooth technology to connect to the Internet and a downloadable mobile application to respond to a child's questions.[38] My Friend Cayla has been the subject to many criticisms for its undisclosed data collection practices[39] as well as its technological design limitations, i.e. the use of Bluetooth instead of Wi-Fi.[40]

For many adults and children, Hello Barbie is the realization of a childhood dream: having a trusted, best friend that is always available to keep company. Hello Barbie can potentially serve as a pedagogical tool and assist children in developing and improving their cognitive skills. She can help a child problem solve and express their thoughts and feelings by utilizing pre-recorded statements and analysis of speech recordings.[41] It puts an exciting spin on playing with dolls, but it also opens the door to several unknowns, as this is one of the first of a likely progeny of smart toys.

Since the release of Hello Barbie, other interactive toys have entered the market. For instance, iconic talking bear Teddy Ruxpin is being revamped and released.[42] The toy is not fully interactive but contains "a motorized mouth"

---

reeds to simulate vocal cords;" Thomas Edison's entry in a 1877 notebook indicating a commercial use for his new phonograph invention being "to make Dolls speak sing cry;" and various products in the 20th century like Dolly Rekord, a doll that spoke nursery rhymes; Chatty Cathy, "a 1959 release from Mattel whose 11 phrases included 'I love you';" and Teddy Ruxpin, "a mid1980s stuffed bear whose mouth and eyes moved as he told stories." Barbie herself gained voice capabilities in1968 with a pull string that enabled her to speak eight short phrases. *Id*.

35 Katie Lobosco, *Talking Barbie is Too 'Creepy' for Some Parents*, CNN MONEY (Mar. 12, 2015), http://money.cnn.com/2015/03/11/news/companies/creepy-hello-barbie/.

36 Vlahos, s*upra* note 1.

37 *See* Roberts, *supra* note 17.

38 The doll records the conversation to "enhance and improve the services for the toys and for other services and products." *See Hello Barbie Security: Part 2—Analysis*, SOMERSET RECON (Jan. 25, 2016), http://www.somersetrecon.com/blog/2016/1/21/hello-barbie-security-part-2-analysis [hereinafter *Hello Barbie Security*].

39 *See supra* Section I.

40 *Hello Barbie Security*, *supra* note 38. Blue-Tooth technology is more vulnerable to hacking and security breaches than Wi-Fi. When a Blue-Tooth-enabled device (such as the Cayla doll) loses connection with its designated mobile device, it could inadvertently pair with an unknown user's device, increasing the risk of the exposure of the doll's owner's personal information to a potential attacker. *Id.*

41 *See* HELLO BARBIE FAQS, *supra* note 3, at 2.

42 *See* Parija Kavilanz, *Iconic '80s Toy Bear Tech Teddy Ruxpin is Back*, CNN MONEY (Sept. 30, 2016), http://money.cnn.com/2016/09/30/technology/teddy-ruxpin-toy-bear/.

and "LCD eyes that show 40 animated expressions synched to the stories."[43] The talking bear also contains an internal hard drive including ten prerecorded stories and the ability to download more.[44] Additionally, Disney Consumer Products and Interactive Media Labs created an interactive Miss Piggy Facebook page, which allows you to Facebook message with the famous character.[45] Miss Piggy's interactive Facebook page takes the old AOL Instant Messenger feature of "Smarter Child" to a new level.[46] The fictional Facebook page is powered by Imperson, a company that creates conversational bots capable of simulating conversations with people.[47]

In its most simplistic view, Hello Barbie is like Siri or Cortana but located in a doll and accessed almost entirely children. She listens to what you or your child says and then uses "breath to bytes"[48] to encode and respond appropriately. The doll requires minimal setup: download the mobile application and connect Barbie to the Internet. Once the doll connects to the Wi-Fi, everything a child says to the doll while pressing Barbie's belt buckle (the record button) is recorded. These recorded statements are then sent to ToyTalk to generate a response from Barbie, and saved in an online data storage cloud.[49] The responses are stored to help create a more "tailored response… [so it] almost

---

43 *Id.*

44 *See id.* ("He can blink and look up and down, but his eyes also flash hearts, stars, even snowflakes.").

45 *See* Drew Olanoff, *Go Chat with Miss Piggy on Facebook Messenger*, TECH CRUNCH (Dec. 7, 2015), https://techcrunch.com/2015/12/07/go-chat-with-miss-piggy-on-facebook-messenger/.

46 *See* Ashwin Rodrigues, *A History of SmarterChild*, VICE: MOTHERBOARD, (Mar. 16, 2016), http://motherboard.vice.com/read/a-history-of-smarterchild. ("SmarterChild was a robot that lived in the buddy list of millions of American Online Instant Messenger (AIM) users." It was a "robot that instantly pulls and returning info from the internet when requested."). *Id.*

47 Conversational bots use natural language processing to interact with others. *See id.*; *see* Annlee Ellingson, *Miss Piggy Talks to Fans Thanks to Imperson's Chat Bot*, BIZ JOURNALS (Feb. 3, 2016), http://www.bizjournals.com/losangeles/news/2016/02/03/miss-piggy-talks-to-fans-thanks-to-imperson-s-chat.html; *see also Conversational Bots for Brands*, IMPERSON, http://imperson.com/ (last visited Nov. 8, 2016).

48 JOHN FRANK WEAVER, ROBOTS ARE PEOPLE TOO: HOW SIRI, GOOGLE CAR, AND ARTIFICIAL INTELLIGENCE WILL FORCE US TO CHANGE OUR LAWS 7 (2014) [hereinafter ROBOTS ARE PEOPLE TOO].

49 Vlahos, s*upra* note 1; *see* Lin, *supra* note 18. The cloud "facilitates the migration of essential computing and storage facilities from local devices owned by users to distant servers owned by providers." When a child records a conversation with Barbie, the recordings are immediately sent to a cloud for virtual storage. The cloud is the most efficient way to keep up with the number of consumers projected to use this toy. It also makes it easier to create big data and analyze the children's responses.

seems like 'she's alive.'"[50] In addition to ToyTalk having access to the recorded conversations through the storage cloud, parents are able to access the conversations and recordings through the mobile application.[51] If a parent or guardian is unhappy with the recorded content, they are able to delete it from the application.[52]

ToyTalk adheres to the FTC's KidSafe Seal Program, a compliance program for websites and online services targeted towards children.[53] There are two types of certificates that a website or online service can obtain: the kidSafe certificate and the kidSAFE+ certificate.[54] To be kidSAFE certified, the website or online service must meet the Basic Safety Rules.[55] The kidSAFE+ certificate requires additional requirements and compliance with COPPA. Because Hello Barbie targets at the age range COPPA protects, ToyTalk not only satisfies the basic kidSAFE requirements but the additional requirements for kidSAFE+. For example, the communications between Hello Barbie and a child are encrypted and stored on a trusted network on the cloud servers.[56] Additionally, Hello Barbie's hardware limits the number of "clients that interface with each other and the cloud."[57] There are three potential clients: the mobile application, which acts as an access point for Wi-Fi for the doll and the corresponding ToyTalk account; Barbie, who communicates with the ToyTalk servers that store and process the data in the cloud; and an Internet browser that communicates with the ToyTalk servers and can access an individual's account with proper credentials such as password and user name.[58] The figure below demonstrates the communication processes between different devices, ToyTalk, and Hello Barbie.

---

50 Griffiths, *supra* note 16.

51 *See id.*

52 *See id.*

53 *See* FEDERAL TRADE COMMISSION, KIDSAFE SEAL PROGRAM: CERTIFICATION RULES-VERSION 3.0 (FINAL) 1 (2014), *available at* https://www.ftc.gov/system/files/attachments/press-releases/ftc-approves-kidsafe-safe-harbor-program/kidsafe_seal_program_certification_rules_ftc-approved_kidsafe_coppa_guidelines_feb_2014.pdf [hereinafter KIDSAFE SEAL PROGRAM].

54 *See id.*

55 *See id*. Basic safety rules: "1. Chat and other interactive community features must be designed with safety protections and controls; 2. Must post rules and educational information about online; 3. Must have procedures for handling safety issues and complaints; 4. Must give parents basic safety controls over their child's activities; 5. Content, advertising, and marketing must be age-appropriate."

56 *Hello Barbie Security*, *supra* note 38.

57 *Id.*

58 *See id.*

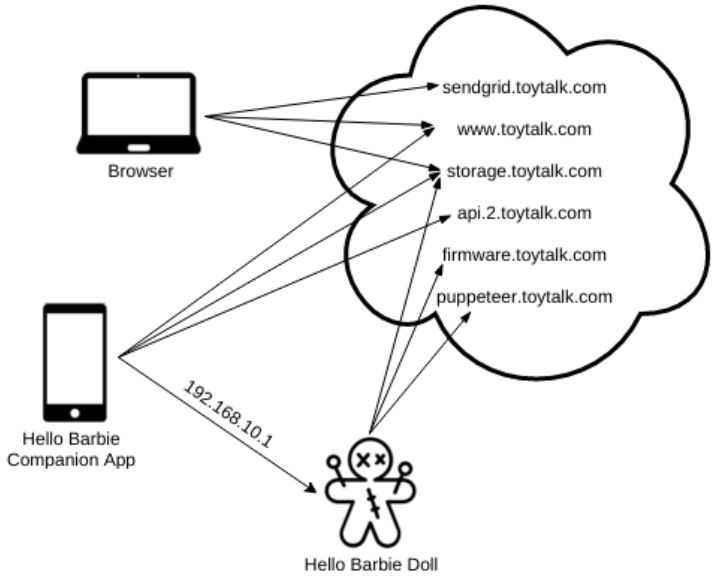

Fig. 1 demonstrating the communication paths between different clients and the cloud server.[59]

B. An Overview of the Internet of Things and Artificial Intelligence

Many of these new smart toys fall under a broader category of "intelligent" devices designed to self-configure and connect to the existing Internet, using a wireless network such as Wi-Fi or Bluetooth technology. Collectively, these smart devices form a new ecosystem referred to as the Internet of Things ("IoT"). [60] The IoT is a rapidly growing "network of physical devices (or 'things')" which is capable of sensing and collecting data about their environment, and transmits that data via the Internet to an online system, such as a cloud.[61] The IoT allows smart devices to easily communicate and exchange data with each other or other external systems and receive commands from external sources by downloading and executing small applications, also known as apps.[62]

To qualify as a *smart* device, these objects must be able to sense and interact with their immediate environment,[63] and communicate with devices or hu-

---

59 *Id.*

60 Antigone Peyton, *A Litigator's Guide to the Internet of Things*, 22 RICH. J. L. & TECH. 9, 9 (2016).

61 *See id.*

62 *See id.* at 11.

63 An example interaction with the environment would be voice commands from a hu-

mans.[64] Many of these devices are equipped with sensors[65] and can record sensor signals (e.g., human conversation), later transmitting the recorded data to other devices or external systems via the Internet.[66] Computer scientists are actively working to develop new methods and technologies to automatically process, categorize, and understand massive amounts of data that are being collected by these devices.[67] In fact, a relatively new branch of Artificial Intelligence ("AI") research, called Machine Learning ("ML"), focuses on developing computer algorithms, which allow machines to process and transform vast amounts of raw data collected by IoT devices into meaningful, actionable information, which can be used by humans.[68] Without advanced ML technologies, vast quantities of information collected by IoT devices are of little tangible value.[69]

Hello Barbie is a prime example of a new wave of smart toys that can interact with their human user. Hello Barbie leverages AI technologies, including natural language processing, to deliver a life-like interactive experience to its human subject. AI is a subfield of computer science[70] that strives to create machines with human-like cognitive capabilities.[71] More specifically, to create machines with the cognitive ability to learn from their past interactions with humans or their environment, process sensed data, and problem solve in a

---

man or the ability to sense movement or motion.

64 *See* Peyton, *supra* note 60, at 12.

65 These devices may be equipped with sensors for sound, video, temperature, motion-detection, etc.

66 *See id.*

67 *See When IoT Meets Artificial Intelligence*, WAYLAY.IO http://www.waylay.io/blog-iot-meets-artificial-intelligence.html (last visited Dec. 13, 2016).

68 *See* Mark Jaffe, *IOT Won't Work Without Artificial Intelligence*, WIRED, https://www.wired.com/insights/2014/11/iot-wont-work-without-artificial-intelligence/ (last visited Dec. 11, 2016).

69 *Id*. (explaining that "the data by themselves do not provide value unless we can turn them into actionable, contextualized information ... Real-time sensor data analysis and decision-making is often done manually but to make it scalable, it is preferably automated. Artificial Intelligence provides us the framework and tools to go beyond trivial real-time decision and automation use cases for IoT.").

70 STUART JONATHAN RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH 18 (3d ed. 2010) (discussing important aspects of A.I.). AI is described as intelligence by machines and through software. Kris Hammond, *What is artificial intelligence*?, COMPUTERWORLD (Apr. 10, 2015), http://www.computerworld.com/article/2906336/emerging-technology/what-is-artificial-intelligence.html.

71 Istvan S.N. Berkeley, *What is Artificial Intelligence?*, UCS LOUISIANA, http://www.ucs.louisiana.edu/~isb9112/dept/phil341/wisai/WhatisAI.html (last visited Mar. 30, 2017).

manner similar to how humans operate.[72] Many of the everyday devices such as home appliances, cellphones, TVs, and online music radios like Pandora and Spotify increasingly incorporate AI technologies.

One of the main objectives of AI design is to create devices and computer systems that can process and learn from their environment, generate plans of action, self-collect information, create knowledge, and operate and communicate autonomously.[73] Experts in the field hope that "intelligent" systems will soon be able to carry out many of the everyday tasks performed by humans but in a more efficient manner.[74] Autonomous, self-driving cars are a prime example of such new developments.[75] Computer scientists and software engineers have not developed the type of AI portrayed in science fiction movies such as Star Wars; however, they have been successful in creating less complex forms of AI that we use daily.[76]

AI falls into two broad categories: strong AI and weak AI. Strong AI refers to a machine's cognitive ability to "match or exceed human intelligence."[77] This means that a machine equipped with strong AI is capable of performing human cognitive tasks such as reasoning and making deductions based on data presented.[78] Weak AI refers to a set of techniques, which allow computers to mimic or recreate the logic abilities of humans.[79] Hello Barbie is an example of a smart device incorporating weak AI. Other common types of weak AI are "Google's search engine, Global Positioning System (GPS), and video games."[80]

For smart devices to be effective, they must be able to accurately process, filter, and analyze the data they collect from their environment, convert raw data into actionable information, and produce appropriate responses. The nature of the data collected varies from device to device and depends on the type of sensors and interactions between a device and its subject. Wearable devices, such as Fitbit, sense and collect intimate personal data, including behavioral and physiological biometrics (i.e., heart rate, physical movements, and sleep

---

72 *See* Hammond, *supra* note 70.

73 *See* Avneet Pannu, *Artificial Intelligence and its Application in Different Areas*, 4 INT'L J. ENG'G & INNOVATIVE TECH. (IJEIT) 79, 79, 84 (2015).

74 *See id.*

75 *See* ROBOTS ARE PEOPLE TOO, *supra* note 48, at 17.

76 *See id.* at 3.

77 *Id.*

78 *See id.*; *see A Holistic Approach to AI*, OCF BERKELEY, https://www.ocf.berkeley.edu/~arihuang/academic/research/strongai3.html (last visited Oct. 31, 2016).

79 *See* RUSSELL & NORVIG, *supra* note 70, at 1020.

80 ROBOTS ARE PEOPLE TOO, *supra* note 48, at 3.

patterns).[81] Other devices, such Amazon Echo and Siri, can record human speech in audio or video format, and are sometimes referred to as communication-capturing technology.[82] Communication-capturing technology has two components: first, that the technology records a user's speech, and second, that the technology encodes the speech and transmits it to a secure remote server hosted by either the manufacturer or a third party,[83] where the transmitted data is stored on the server indefinitely.[84]

Consider Siri, the popular voice assistant included with the iPhone. Siri is a prominent example of an AI-enabled consumer technology incorporated into a common device. It is also one of the first forms of AI to actually be mass marketed as artificial intelligence.[85] Siri is a product of a six-year collaboration between DARPA (Defense Advanced Research Projects Agency) and SRI International, a research group in Menlo Park, California, to create a "cognitive assistant that learns and organizes."[86] It uses speech for both input and output, allowing users to communicate with it and receive a response.[87] Siri was eventually bought by Apple and was released in its iPhone 4S.[88] The virtual assistant sends commands via remote server to encode speech, analyze it, and respond.[89]

More specifically, Siri encodes your speech and transforms it into a compact digital form that is swiftly transmitted via cellular signals to Internet service providers who then send it to a cloud-based remote server.[90] Once the encoded speech is on the server, the speech is analyzed and evaluated to determine the proper response to such a command.[91] If the command cannot be "handled on

---

81 *See* Mark Weinstein, *What Your Fitbit Doesn't Want You To Know*, HUFFINGTON POST (Dec. 21, 2015), http://www.huffingtonpost.com/mark-weinstein/what-your-fitbit-doesnt-w_b_8851664.html.

82 *See* Alex B. Lipton, *Privacy Protections for Secondary Users of Communications-Capturing Technologies*, 91 N.Y.U. L. REV. 396, 397 (2016).

83 *See id.* at 400.

84 Some companies periodically delete stored data or the data may be removed from the server if the user cancels its service or account.

85 *See* John Weaver, *Siri is my Client: A First Look at Artificial Intelligence and Legal Issues*, 52 N.H. B.J. 6, 6 (2012).

86 *Id*.

87 *See id.*; *see* Timothy Hay, *Apple Moves Deeper Into Voice-Activated Search With Siri Buy*, WALL ST. J. BLOG (Apr. 28, 2010, 1:17 PM), http://blogs.wsj.com/venturecapital/2010/04/28/apple-moves-deeper-into-voice-activated-search-with-siri-buy/.

88 *See* Jill Duffy, *What is Siri?*, PC MAGAZINE (Oct. 17, 2011), http://www.pcmag.com/article2/0,2817,2394787,00.asp.

89 *See* ROBOTS ARE PEOPLE TOO, *supra* note 48, at 4–5.

90 *See* Weaver, *supra* note 85, at 4.

91 *See id.*

the phone… [and] the server is needed it will compare your speech with a data-based model to estimate what letters might constitute it. The server then uses the highest-probability estimate to proceed."[92]

Before Siri can produce a response, your speech, which is currently in the form of vowels and consonants, is analyzed to determine the specific words. "The computer then creates a list of likely interpretations for what your speech might mean and chooses the most probable. If there is enough confidence in this result, it will complete your command."[93] If Siri cannot understand the speech because it is vague, Siri will respond with some variation of "Sorry, I didn't get that."[94] This whole process takes approximately three seconds and becomes more efficient over time as Siri continues to collect data from its users.[95]

With the rapid proliferation of newer, more capable, and increasingly "smarter" devices, the collection of personal data has become a serious privacy concern. New devices are being designed to deliver greater convenience, ease of use, and enjoyment to the consumer. In return, these devices are becoming more intrusive in the manner in which they sense and collect information about their environment. The question then becomes, what do these companies do with the collected data? The following section will examine this issue and introduce the concept of duty to report and its implications for smart devices and their manufacturers.

C. Data Collection and the Duty to Report

Data collection and the Internet of Things are popular aspects of businesses today. Many companies have adopted business frameworks that involve consumer data collection in addition to offering a free product or service.[96] Many companies use the data collected to update and modify their product or service, while others sell this data to third party advertisers and marketers.[97] Social media giants like Google and Facebook are notorious for such data practices, and justify mass data collection by providing a quality service, free of charge,

---

92 *See id.*

93 *See id.*

94 *See id.*

95 *See* Duffy, *supra* note 88.

96 Ira Winkler, *Facebook is Not Free*, COMPUTERWORLD (Oct. 17, 2011), http://www.computerworld.com/article/2499036/web-apps/facebook-is-not-free.html.

97 In some instances, these companies must give courts access to this personal information as well. *See* Allied Concrete Co. v. Lester, 736 S.E.2d 699, 702 (Va. 2013) (using previous Facebook posts to show that Lester deleted relevant information to prevent the opposing counsel from getting access during discovery).

without pop-up advertisements and spam.[98] Many consumers remain unfazed by this intrusion of privacy, and fall victim to the price of free.[99] Many legal issues arise with data collection, such as unfair data collection practices, secureness of the data collected and stored, and the analysis of the data collected. The remainder of this section focuses on legal concerns regarding the analysis of data collected and introduces the common law duty to report. This duty to report is triggered in specific situations outlined in state law.

Data collection has been used in statistical analysis since the 1960s, but it was not used commercially until the 1980-1990s, when database marketing became a popular advertising tool.[100] Database marketing encourages companies to utilize the large quantities of collected consumer information to strategically advertise and promote products.[101] Companies analyze consumer data to predict "how likely you are to buy a product and use that knowledge to craft a marketing message precisely calibrated"[102] to get the consumer to purchase the product. Database marketing demonstrates very little regard for consumers' privacy but it remains a strong marketing tool today.[103]

The collected data includes basic personal information such as name, location, IP address, and email address; but it also includes an individual's Internet behavior.[104] This type of data collection is referred to as online behavioral tracking, because an individual's browsing activity is compiled and made into a profile, which marketers and advertisers use to market specific services and products.[105] A newer and more invasive trend is to capture recorded speech and

---

98 *See* Winkler, *supra* note 96; *see* Mark Hachman, *The Price of Free: How Apple, Facebook, Microsoft and Google Sell you to Advertisers*, PCWORLD (Oct. 1, 2015), http://www.pcworld.com/article/2986988/privacy/the-price-of-free-how-apple-facebook-microsoft-and-google-sell-you-to-advertisers.html.

99 *See* Sunday Yokubaitis, *You are the Product: The Price of Free in the Growing Privacy Industry*, LINKEDIN (Jan. 12, 2016), https://www.linkedin.com/pulse/you-product-price-free-growing-privacy-industry-sunday-yokubaitis.

100 *See* Gil Press, *A Very Short History of Data Science*, FORBES (May 28, 2013), http://www.forbes.com/sites/gilpress/2013/05/28/a-very-short-history-of-data-science/#531edca269fd; *see* Jonathan Berry, *Database Marketing*, BLOOMBERG (Sept. 5, 1994), http://www.bloomberg.com/news/articles/1994-09-04/database-marketing.

101 *See id.*

102 Berry, *supra* note 100 (discussing "an earlier flush of enthusiasm prompted by the spread of checkout scanners in the 1980s ended in widespread disappointment.").

103 *See id.*

104 ELECTRONIC FRONTIER FOUNDATION, ONLINE BEHAVIORAL TRACKING AND TARGETING LEGISLATIVE PRIMER 13 (2009), https://www.eff.org/files/onlineprivacylegprimersept09.pdf.

105 *See* David R. Hostetler & Seiko F. Okada, *Children's Privacy in Virtual K-12 Education: Virtual Solutions of the Amended Children's Online Privacy Protection Act (COPPA) Rule*, 14 N.C. J.L. & TECH. ON. 167, 171–72 (2013).

video.[106] Products like Hello Barbie, the Samsung Smart TV, Siri, and Amazon Echo capture a user's speech and/or video and store it on a server to later analyze.[107] Companies that review this recorded speech and/or video have the potential to obtain significantly more personal information and data about its consumers. Yet these companies are very rarely required to report any suspicious speech or video they may find—that is unless the makers of Amazon Echo or Samsung Smart TV fall under the common law duty to report. Any other duty to report suspicious speech or video would be outlined in the company privacy policy; however it is highly unlikely a company will self-impose such a duty. Below is a brief description of the common law duty to report. Such an analysis is necessary as these companies engage in mass data collection. The more data collected, the more likely there is recorded speech that should be reported.

The duty to report arises from United States common law. There are many subsets of the duty to report, which include reporting known or suspected child abuse and neglect.[108] All fifty states and territories "have statutes identifying persons who are required to report suspected child maltreatment to an appropriate agency, such as child protective services, a law enforcement agency, or a State's toll-free child abuse reporting hotline."[109] The vast majority of states (and territories) designate specific individuals that are required to report suspected child abuse and neglect. These designated individuals include: social workers; teachers, principals, and other school personnel; physicians, nurses, and other health-care workers; counselors, therapists, and other mental health professionals; child care providers; medical examiners or coroners; and law enforcement officers.[110]

Additionally, some states require reporting from commercial film or photograph processors,[111] computer technicians,[112] substance abuse counselors,[113]

---

106 *See, e.g.*, Chris Matyszszyk, *Samsung's Warning: Our Smart TVs Record your Living Room Chatter*, CNET (Feb. 8, 2015), https://www.cnet.com/news/samsungs-warning-our-smart-tvs-record-your-living-room-chatter/ (discussing the new privacy threats with communication-capture technology utilized in Samsung's Smart TV).

107 *See* HELLO BARBIE FAQS, *supra* note 3, at 4–5.

108 *See* Alison M. Arcuri, *Sherrice Iverson Act: Duty to Report Child Abuse and Neglect*, 20 PACE L. REV. 471, 474, 489 (2000).

109 MANDATORY REPORTERS OF CHILD ABUSE AND NEGLECT, *supra* note 14, at 1.

110 *Id.* at 2.

111 "Film processors are mandated reporters in [Puerto Rico, Guam,] Alaska, California, Colorado, Georgia, Illinois, Iowa, Louisiana, Maine, Missouri, Oklahoma, South Carolina, and West Virginia." *See id.*

112 "Computer technicians are required to report in Alaska, California, Illinois, Missouri, Oklahoma, and South Carolina." *See id.*

113 "Substance abuse counselors are required to report in Alaska, California, Connecticut, Illinois, Iowa, Kansas, Massachusetts, Nevada, New York, North Dakota, Oregon, South

probation officers,[114] and workers at "entities that provide organized activities for children."[115] In several states, these designated individuals are the only persons required to report child neglect and abuse. However, in eighteen states and Puerto Rico, any person who suspects child abuse or neglect is required to report.[116] New Jersey and Wyoming are the only states "that require all persons to report without specifying any profession. In all other states, territories, and the District of Columbia, any person is permitted to report."[117] Thus, for a child a like Tiara, ToyTalk may only have a duty to report if she lives in one of the eighteen states that require any person who suspects child abuse or neglect to report. Setting aside the potential conflicts of law issues that may arise if the child using Hello Barbie is located in a state other than California, let us consider one state's laws in particular, California, as ToyTalk is headquartered there.[118]

California only imposes a mandatory duty to report on specific professionals; all other persons "may report."[119] The state law includes computer technicians as a mandatory reporter.[120] Section 11166(e)(2) requires commercial computer technicians "who ha[ve] knowledge of or observe[], within the scope of his or her professional capacity or employment, any representation of information, data, or an image…shall immediately, or as soon as practicably possible, telephonically report the instance of suspected abuse to the law enforcement agency."[121] Computer technicians include any person who works in the computer repair or servicing industry, such that the technician may have access to the computer, its memory, and any saved or marked files or internet searches. A computer technician may also have access to the "recording mechanism, auxiliary storage recording or memory capacity, or any other material

---

Carolina, South Dakota, and Wisconsin." *See id.*

114 *See* MANDATORY REPORTERS OF CHILD ABUSE AND NEGLECT, *supra* note 14, at 2 ("Probation or parole officers are mandated reporters in Arkansas, California, Colorado, Connecticut, Hawaii, Illinois, Louisiana, Massachusetts, Minnesota, Missouri, Nevada, North Dakota, South Dakota, Texas, Vermont, Virginia, and Washington.").

115 *Id.* ("Directors, employees, and volunteers at entities that provide organized activities for children, such as camps, day camps, youth centers, and recreation centers, are required to report in…California, Hawaii, Illinois, Louisiana, Maine, Nevada, New York, Ohio, Oregon, Pennsylvania, Vermont, Virginia, and West Virginia.").

116 These states are Delaware, Florida, Idaho, Indiana, Kentucky, Maryland, Mississippi, Nebraska, New Hampshire, New Mexico, North Carolina, Oklahoma, Rhode Island, Tennessee, Texas, and Utah. *See id.*

117 *Id.*

118 ToyTalk is headquartered in San Francisco, California. *See Contact*, TOYTALK, https://www.toytalk.com/about/contact/ (last visited Dec. 12, 2016).

119 CAL. PENAL CODE § 11165.7 (2016)

120 *See id.* § 11165.7 (a)(43)(A)-(B).

121 *Id.* § 11166(e)(2).

relating to the operation and maintenance of a computer or computer network system, for a fee."[122] Any company that offers "remote computing services" or "electronic communication services" may also fall under this designation.[123] It is important to note that the computer technician designation along with the commercial film and photographic print or image processor[124] mandatory reporter designation is targeting child pornography.[125]

Even though the computer technician designation of California's duty to report law is rather broad, it is unclear if a company such as ToyTalk would be considered a mandatory reporter. The employees at ToyTalk have many re-

---

122 *Id.* §§ 11165.7 (a)(43)(A)-(B). The statute defines computer technician as "(A) a person who works for a company that is in the business of repairing, installing, or otherwise servicing a computer or computer component, including, but not limited to, a computer part, device, memory storage or recording mechanism, auxiliary storage recording or memory capacity, or any other material relating to the operation and maintenance of a computer or computer network system, for a fee. An employer who provides an electronic communications service or a remote computing service to the public shall be deemed to comply with this article if that employer complies with Section 2258A of Title 18 of the United States Code. (B) An employer of a commercial computer technician may implement internal procedures for facilitating reporting consistent with this article. These procedures may direct employees who are mandated reporters under this paragraph to report materials described in subdivision (e) of Section 11166 to an employee who is designated by the employer to receive the reports. An employee who is designated to receive reports under this subparagraph shall be a commercial computer technician for purposes of this article. A commercial computer technician who makes a report to the designated employee pursuant to this subparagraph shall be deemed to have complied with the requirements of this article and shall be subject to the protections afforded to mandated reporters, including, but not limited to, those protections afforded by Section 11172.".

123 18 U.S.C. § 2258A (2008); *see Congress Passes New Rules for Child Pornography Reporting by ISPs*, LEXOLOGY (Oct. 22, 2008), http://www.lexology.com/library/detail.aspx?g=f7bc565c-a046-4470-9503-4140e42d29b7 (discussing the PROTECT Our Children Act, "which expands existing child pornography reporting requirements and enhances the government's ability to prosecute producers and traffickers of child pornography.").

124 This mandatory reporter includes "a commercial film and photographic print or image processor as specified in subdivision (e) of Section 11166." As used in this article, "commercial film and photographic print or image processor" means a person who develops exposed photographic film into negatives, slides, or prints, or who makes prints from negatives or slides, or who prepares, publishes, produces, develops, duplicates, or prints any representation of information, data, or an image, including, but not limited to, any film, filmstrip, photograph, negative, slide, photocopy, videotape, video laser disc, computer hardware, computer software, computer floppy disk, data storage medium, CD-ROM, computer-generated equipment, or computer-generated image, for compensation. The term includes any employee of that person; it does not include a person who develops film or makes prints or images for a public agency." *See* PENAL § 11165.7 (a)(29).

125 *See* A.B. 1817, 2011-12 Reg. Sess. (2012) (amended) (defining pornography as "depicting a child under 16 years of age engaged in an act of sexual conduct.").

sponsibilities, including reviewing the recorded speech to help improve Barbie. ToyTalk employees who are charged with such tasks should be considered mandatory reporters because of their direct access to such personal and intimate conversations. Part IV of this article further discusses the implications if the ToyTalk employees are not classified under the computer technician. After concluding that these employees would not be classified as a computer technician, Section IV proposes an appropriate to solution to such a problem,

PRIVACY LAW IN THE COMPUTER AGE

It is widely accepted that the development of privacy laws lags behind the speed of technological innovation. In fact, there are only a handful of federal privacy laws that apply to certain aspects of artificial intelligence and data collection—the bulk of protection comes from state law and regulations.[126] The United States takes a very different patchwork approach to privacy law, unlike many other industrialized nations or the European Union, which provides all-encompassing protection.[127] This patchwork approach leaves certain areas and industries unprotected and unregulated.[128] Intelligent toys such as Hello Barbie are one of those sectors. This section identifies and describes the relevant privacy laws regarding smart toys such as Hello Barbie. This section also introduces the common law duty to report laws and further discusses the gap identified above.

The need for privacy and data security laws arose after the advent of personal computers and the information technology boom of the 1990s.[129] As technology advanced "few laws directly regulated privacy [concerns] in many of these contexts."[130] Attempts to use existing privacy tort laws and statutory laws such

---

126 "Today, we have hundreds of laws pertaining to privacy: the common law torts, criminal law, evidentiary privileges, constitutional law, at least twenty federal statutes, and numerous statutes in each of the fifty states." *See* Daniel J. Solove, *A Brief History of Information Privacy Law*, GWU L. FAC. PUB. & OTHER WORKS 1-3 (2006), http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications [hereinafter *A Brief History of Information Privacy Law*].

127 *See* Daniel J. Solove, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014) ("Unlike the privacy laws of many industrialized nations, which protect all personal data in an omnibus fashion, privacy law in the United States is sectoral, with different laws regulating different industries and economic sectors.").

128 *See id.* (discussing implications of patchwork protection. "For example, there is no federal law that directly protects the privacy of data collected and used by merchants such as Macy's and Amazon.com. Nor is there a federal law focused on many of the forms of data collection in use by companies such as Facebook and Google. Most state laws are ineffective at addressing these problems, as are the four privacy torts.").

129 *See id.* at 590.

130 *See id.*

as the Electronic Communication Privacy Act ("ECPA") were fruitless and ill-fitting, because the laws were designed to regulate wiretapping and eavesdropping rather than the data collection processes of commercial entities.[131] In the late 1990s and early 2000s, two schools of thought emerged regarding privacy laws.[132] One set of commentators suggested that the Internet and technology would be stunted by the implementation of a regulatory scheme.[133] More specifically, these commentators suggested that these industries were best suited to be self-regulating regimes, providing notice of existing privacy policies and terms and conditions for its customers.[134] The other school of thought was that the United States needed stronger privacy law protection, suggesting that those who promoted self-regulation did not understand the benefits of the law nor did they understand the difference between "cyberspace transactions" and regular transactions.[135] Furthermore, the self-regulation commentators "overemphasize the differences between cyberspace transactions and other transactions," the commentators do not understand the "basic differences between default laws and mandatory laws," and finally they underestimate the potential of legal tools to solve "potential multijurisdictional problems."[136] These two

131 *See id.* at 591; *see also, e.g., In re* DoubleClick, Inc. Privacy Litigation, 154 F. Supp. 2d 497, 507 (S.D.N.Y. 2001). (discussing how plaintiffs failed to challenge use of cookies under the ECPA. The court dismissed the case on the grounds that "DoubleClick-affiliated Web sites consented to DoubleClick's access of plaintiffs' communications to them." The ECPA was indeed a poor fit, as it was designed to regulate wiretapping and electronic snooping rather than commercial data gathering. The records maintained by Internet retailers and websites were often held not to be "communications" under the ECPA.).

132 *See* Amy Lynne Bomse, *The Dependence of Cyberspace*, 50 DUKE L. J. 1717, 1719 (2001).

133 *See id.*

134 *See* Solove, *supra* note 127, at 592–93.

135 *See* Bomse, *supra* note 132, at 1719 (discussing the other school of thought, "Professor Lawrence Lessig's book Code is certainly the most prominent of such critiques. Lessig argues that digital libertarians are blind to the way the Internet is moving towards an architecture of control."); *see also* Thomas H. Davenport, *Should the U.S. Adopt European Style Data-Privacy Protections?*, WALL ST. J. (Mar. 10, 2013), http://www.wsj.com/articles/SB10001424127887324338604578328393797127094; Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1199-201 (1998).

136 *Id.* at 1199-201. "The skeptics make three basic errors. First, they overstate the differences between cyberspace transactions and other transnational transactions. Both involve people in real space in one territorial jurisdiction transacting with people in real space in another territorial jurisdiction in a way that sometimes causes real-world harms. In both contexts, the state in which the harms are suffered has a legitimate interest in regulating the activity that produces the harms. Second, the skeptics do not attend to the distinction between default laws and mandatory laws. Their ultimate normative claim that cyberspace should be self-regulated makes sense with respect to default laws that, by definition, private parties can modify to fit their needs. It makes much less sense with respect to mandatory or

schools of thought exist today as the United States struggles to keep up with international privacy laws as well as new technological innovations.[137] The remainder of this section identifies privacy laws relevant to Hello Barbie. It begins with common law protections and ends with the most relevant federal statute COPPA.

A. Common Law Privacy Torts

This section provides a brief description of the relevant common law privacy torts. These torts are state law, meaning that there may be variations from state to state.[138] Additionally, these tort laws provide little relief for users of artificial intelligence such as Hello Barbie. Prior to the twentieth century, privacy laws provided limited protection for government records, mail, telegraph communications, and privacy of the body.[139] The Third, Fourth, and Fifth Amendments were created in response to "excessive government power to invade the privacy of the people."[140] Subsequent legislation, new court decisions, and constitutional amendments had little effect on the status of U.S. privacy law.[141] It was not until the 1890s when the right to personal privacy was substantially developed.[142]

In 1890, Samuel Warren and Louis Brandeis released a revolutionary article called "The Right to Privacy."[143] The article proposed that privacy law and protections be extended to include new types of media such as newspapers and

---

regulatory laws that, for paternalistic reasons or in order to protect third parties, place limits on private legal ordering. Third, the skeptics underestimate the potential of traditional legal tools and technology to resolve the multijurisdictional regulatory problems implicated by cyberspace. Cyberspace transactions do not inherently warrant any more deference by national regulators, and are not significantly less resistant to the tools of conflict of laws, than other transnational transactions."

137 *See, e.g.*, Abraham Newman, *After Safe Harbor: Bridging the EU-U.S. Data-Privacy Divide*, WORLD POL. REV. (Feb. 9, 2016), http://www.worldpoliticsreview.com/articles/17898/after-safe-harbor-bridging-the-eu-u-s-data-privacy-divide (discussing the potential changes that must occur to U.S. privacy law after the changes to the safe harbor rule).

138 *A Brief History of Information Privacy Law*, *supra* note 126, at 1-14. ("The most recent state to do so was Minnesota in Lake v. Wal-Mart Stores, Inc., where the state Supreme Court finally recognized the Warren and Brandeis torts in 1998.").

139 *See id.* at 1-4.

140 *Id.* at 1-5.

141 *See id.* Note there were amendments to the Fourth and Fifth Amendments in the late 1800s, which created the protection of a person's papers and personal information. A 1891 Supreme Court created the "privacy of the body."

142 *See id.* at 1-10.

143 *Id.*

cameras.[144] Warren and Brandeis also argued and demanded that new laws be created to protect privacy because current common law and property law fail to do so.[145] The Warren and Brandeis article heavily influenced current privacy torts (including a tort for confidentiality).

The Second Restatement of Torts identifies four main categories of privacy torts.[146] These categories include (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) false light or "publicity"; and (4) appropriation.[147] In addition, to the privacy torts, there is a confidentiality tort that "protect[s] disclosures of information in violation of trust within certain relationships."[148] This tort applies when there is a breach of confidentiality.

Unfortunately, neither the privacy torts nor the confidentiality tort provides adequate protection for the privacy implications of AI and data collection discussed in this article. In fact, previous attempts to apply the privacy torts were struck down by the courts as insufficient. For example, in *Dwyer v. American Express Co.*, the court held that company did not violate the privacy tort of appropriation by selling cardholder names to third parties, because "the defendant's practice [did] not deprive any of the cardholders of any value their individual names may possess."[149] Similarly, in *Shibley v. Time, Inc.*, the court rejected a claim for appropriation against Time magazine who sold its subscription lists to marketers.[150]

The three remaining privacy torts and the confidentiality tort also have had little success. The intrusion upon seclusion tort primarily applies to eavesdropping and unlawful surveillance.[151] Since parents authorize the use of Barbie and her recording feature, this tort does not apply to Hello Barbie. Similarly, the public disclosure of private facts tort only applies to disclosure of private facts illegally obtained.[152] Further, such disclosure must be "widespread." This does not cover cases of personal data collection.[153] The false light tort and confidentiality tort have little relevance because consumers of toys like Hello Barbie have already given up many of their rights to information and confidentiality

144 *Id.*

145 *Id.*

146 *Id.*

147 *Id.* at 1-14.

148 *Id.* at 1-17.

149 *See* Solove, *supra* note 127, at 591–92.

150 *See id.*; *see also* Shibley v. Time, Inc., 341 N.E.2d 337, 339 (Ohio Ct. App. 1975).

151 *See* RESTATEMENT (SECOND) OF TORTS § 652B (Am. Law Inst. 1965).

152 *See id.* § 652D.

153 Solove, *supra* note 127, at 587; *see In re* DoubleClick, Inc. Privacy Litigation, 154 F. Supp. 2d 497, 507 (S.D.N.Y. 2001).

by agreeing to the company's privacy policy.[154] False light and confidentiality may be triggered in situations where the toy is hacked and manipulated publicly;[155] however, it provides little protection for the privacy issues implicated in this article.

B. Contractual Protections

Another form of protection for consumers is contractual privacy policies provided by the seller. This section provides a general description of privacy policies and what protection such policies provide to its consumers. Many privacy policies, including Hello Barbie's privacy policy, include specific references to relevant statutes like COPPA, to provide notice of compliance with such statutes.

Contractual protections such as privacy policies emerged in the 1970s from the Fair Information Practice Principles ("FIPPs").[156] FIPPs are "a set of internationally recognized practices for addressing the privacy of information about individuals."[157] FIPPs provide guidance on various aspects of privacy law such as "an individual's right to have notice about data"[158] collection and an individual's right to consent.[159] These two FIPPS in particular "became the backbone of the U.S. self-regulatory approach, with privacy policies seeking to satisfy the right to notice, and with user choice seeking to satisfy the right to consent."[160]

Today, almost all companies have a terms of service contract as well as a separate privacy policy. This is partially due to state requirements, but also to provide users adequate notice of data collection.[161] These contractual protec-

---

154 *See* RESTATEMENT (SECOND) OF TORTS § 652E; *see* RESTATEMENT (SECOND) OF TORTS § 652C.

155 *See* David Moye, *Talking Doll Cayla Hacked to Spew Filthy Things (UPDATE)*, HUFFINGTON POST (Feb. 9, 2015), http://www.huffingtonpost.com/2015/02/09/my-friend-cayla-hacked_n_6647046.html (discussing the My Friend Cayla hack where the doll said lines from Hannibal Lector and 50 Shades of Grey); *See* RESTATEMENT (SECOND) OF TORTS § 652E.

156 *See* Solove, *supra* note 127, at 592–93.

157 *See* Robert Gellman, *Fair Information Practices: A Basic History* 1 (2016), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

158 *See* Solove, *supra* note 127, at 593.

159 *See id.*

160 *Id.*

161 *See* Lipton, *supra* note 82, at 403 (discussing how some states, such as California, require privacy policies. "Widespread adoption of privacy policies may be due to the fact that California requires privacy policies for any company which collects the personal information of California residents, effectively setting a default requirement for any major website or data-capturing technology.").

tions are considered by many experts to be the first level of protection for users. Privacy policies generally outline what personal information is obtained and stored by the company. These policies are created internally by the companies, but are often restricted due to reputational constraints.[162] More specifically, companies are unlikely to hold data collection practices that are unfavorable to the public and government. Consumers accepting such privacy policies generally have no bargaining power against pro-seller policies. Further, many consumers do not even read these policies in full.[163]

Despite the unequal bargaining power, privacy policies do extend protections to consumers. On the front end, privacy policies provide consumers a "notice and choice" option. This option provides consumers "notice of a privacy policy's terms" by allowing them to "either choose to exit the commercial relationship or continue if they do not find the terms objectionable."[164] These protections are available to the consumer whether or not they read the privacy policy—however the option to exit is not. If they do not read the policy, the consumer will remain unaware of what information is being collected, ultimately weakening this front end protection.[165] Privacy policies also provide protection on the back end. More specifically, "if a seller violates its product's privacy policy by using data in a way that does not accord with the policy's terms, buyers can bring a breach of contract claim, thereby providing buyers with a form of back-end protection as well."[166] Unfortunately, contract-based claims are generally unsuccessful because the consumer is unable to demonstrate specific damages from the breach of privacy policy.[167]

C. Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act ("COPPA") is most applica-

---

162 *Id.* ("While reputational constraints may limit the extent to which companies engage in unpopular data practices, in principle, companies that adopt privacy policies have nearly complete control over what terms to include, and can thus include terms that would offend even the least privacy-focused consumer.").

163 *See* Ian Ayres & Alan Schwartz, *The No-Reading Problem in Consumer Contract Law*, 66 STAN. L. REV. 545, 546 (2014) ("Consumers seldom read the form contracts that firms offer."); *see* Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEGAL STUD. 1, 19, 22 (2014) (providing empirical evidence in support of the argument that consumers seldom read end-user license agreements, and finding that only six per every 1000 retail shoppers read the agreements).

164 *See* Lipton, *supra* note 82, at 404.

165 *See id.*

166 *Id.* at 405.

167 *See id.*

ble to Hello Barbie. The Act was passed in Congress in 1998 and it was designed to address concerns regarding children's privacy.[168] Prior to 1998, there were no protections for minors' personal information.[169] COPPA "prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet."[170] It applies to and protects children under the age of thirteen.[171]

The Act requires that operators of websites targeted at children and that collect personal information from such children to: (1) provide notice of personal information collection policies; (2) obtain parental consent before collecting any personal information; (3) allow parental review of information-gathering practices; (4) prohibit unconditional collection of personal information; and (5) impose reasonable security measures.[172]

Operators are broadly defined under COPPA as "any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained…for commercial purposes."[173] This broad definition encompasses kids' websites like Neopets[174] and Nick[175] as well as Hello Barbie because it utilizes Wi-Fi and cloud-based servers to store and analyze the recorded speech and personal information of minors. In fact, Hello Barbie's privacy policy, which is discussed in Part IV, expressly complies with COPPA. For example, it expressly limits the transfer of data to third parties to comply with COPPA. Fur-

---

168 *See* Hostetler & Okada, *supra* note 105.

169 *See id.* ("A survey by the FTC in 1998 demonstrated that eighty-nine percent of websites for children collected child users' personal data including names, e-mail addresses, postal addresses, phone numbers, fax numbers, and social security numbers. Only twenty-four percent of websites, however, posted privacy statements and only one percent required proof of parental consent for a child to use the website.").

170 Children's Online Privacy Protection Rule, 16 C.F.R. § 312.1 (2001); *see* Daniel Patrick Graham, *Public Interest Regulation in the Digital Age*, 1 COMMLAW CONSPECTUS 97, 124 (2003).

171 *See* 15 U.S.C. § 6501(1) (2016).

172 *See id.* § 6502; *see also* Hostetler & Okada, *supra* note 105, at 177. COPPA was amended in 2012 to keep up with technological innovation. The amended Act: "1) expands the definition of "personal information;" (2) expands the definition of "operators" covered by COPPA; (3) expands COPPA coverage to third parties who collect personal information through web operators; (4) redefines existing exemptions to COPPA regulation; (5) redefines methods to obtain verifiable parental consent; (6) strengthens parental notice requirements; (7) requires reasonable procedures to ensure confidentiality and security during data retention and deletion; and (8) strengthens the FTC's oversight of self-regulatory "safe harbor" programs." *See id.* at 184 n. 112-20.

173 15 U.S.C. § 6501(2).

174 *See* NEOPETS, www.neopets.com (last visited Nov. 5, 2016).

175 *See* NICK, www.nick.com (last visited Nov. 5, 2016).

ther, the Hello Barbie mobile companion application requires parental consent after viewing the doll's privacy policy and terms of service. If Hello Barbie or any another operator fails to satisfy the five requirements, above the operator may face state civil actions as well as civil penalties from the Federal Trade Commission ("FTC").[176]

D. California's Privacy Rights for California Minors in the Digital World

The state of California has been unofficially deemed to have "the nation's best digital privacy laws."[177] California provides rigorous privacy and data security protections for consumers that go beyond federal law.[178] One California law is particularly relevant to the privacy issues highlighted in this article, the Privacy Rights for California Minors in the Digital World.[179] This state law expands federal law, specifically COPPA, and prohibits an online website provider from certain types of advertising and marketing practices.[180] The law also restricts a company's ability to sell or disclose the personal information of a minor.[181] Additionally, the bill requires the "operator to provide notice to a mi-

---

176 *Id*. § 6502(c); *see* Unfair or Deceptive Act of Practices Rulemaking Proceedings, 15 U.S.C. § 57a(a)(1)(B) (2012).

177 Kim Zetter, *California Now Has the Nation's Best Digital Privacy Laws*, WIRED (Oct. 8, 2015), https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/.

178 *See id.*

179 *See* CAL. BUS. & PROF. CODE § 22580, et seq. (2016).

180 *Id.*; S.B. 568, Reg. Sess. 2015 (Pa. 2016) (stating that this bill would "prohibit an operator of an Internet Web site, online service, online application, or mobile application, as specified, from marketing or advertising specified types of products or services to a minor. The bill would prohibit an operator from knowingly using, disclosing, compiling, or allowing a 3rd party to use, disclose, or compile, the personal information of a minor for the purpose of marketing or advertising specified types of products or services. The bill would also make this prohibition applicable to an advertising service that is notified by an operator of an Internet Web site, online service, online application, or mobile application that the site, service, or application is directed to a minor. The bill would, on and after January 1, 2015, require the operator of an Internet Web site, online service, online application, or mobile application to permit a minor, who is a registered user of the operator's Internet Web site, online service, online application, or mobile application, to remove, or to request and obtain removal of, content or information posted on the operator's Internet Web site, service, or application by the minor, unless the content or information was posted by a 3rd party, any other provision of state or federal law requires the operator or 3rd party to maintain the content or information, or the operator anonymizes the content or information. The bill would require the operator to provide notice to a minor that the minor may remove the content or information, as specified.").

181 *See* BUS. & PROF. CODE § 22580.

nor that the minor may remove the content or information, as specified."[182] This privacy law provides more protection for children over the age of thirteen who are no longer protected under COPPA.

E. The "Gap"

The previous sections demonstrate that the current patchwork of privacy regulations and statutes target specific aspects of new technologies but neglect other aspects and industries. Even effective statutes such as COPPA fall short. COPPA imposes effective notice and consent requirements to provide protections for children under the age of thirteen. However, the federal statute does not provide protection for children over the age of thirteen, nor does it truly regulate the collection of a minor's recorded speech.[183] COPPA prohibits the unconditional collection of personal data, but it does not provide specific limitations.[184] The purpose of the Act is to ensure that parents and guardians are provided with accurate notice of what data is being collected and what is being done with it, while depending on other state and federal laws to fill in the holes. Unfortunately, there is no state law or federal law that addresses the gap identified in this article. This gap requires companies like ToyTalk and its employees to be mandatory reporters of suspected child abuse and neglect. Existing duty to report laws are not sufficient, as only eighteen states require all persons to report suspected abuse and neglect.[185] This leaves children like Tiara helpless in 32 other states.[186]

The "gap" gives companies too much autonomy when handling a minor's recorded speech. Smart toy manufacturers are able to review recorded speech at their convenience with very little regulation. Further, such companies are able to delete any additional personal information provided to them and do nothing else.

ANALYSIS: HOW TO BRIDGE THE GAP

Part IV of this article aims to bridge the "gap." Section A analyzes Hello

---

182 S.B. 568, Reg. Sess. 2015 (Pa. 2016).

183 COPPA prohibits the unconditional collection of personal information, but that is it.

184 *See* 15 U.S.C. § 6502 (2016).

185 MANDATORY REPORTERS OF CHILD ABUSE AND NEGLECT, *supra* note 14, at 2 (including "Delaware, Florida, Idaho, Indiana, Kentucky, Maryland, Mississippi, Nebraska, New Hampshire, New Mexico, North Carolina, Oklahoma, Rhode Island, Tennessee, Texas, and Utah.").

186 *See id.* However, in Alaska, Illinois, Missouri, Oklahoma, and South Carolina companies like ToyTalk may fall under the computer technician designation and be considered a mandatory reporter.

Barbie's privacy policy to determine if a child, such as Tiara, would be protected by any self-imposed notice or reporting requirements. With little protection in the privacy policy, Section B turns back to the definition of the computer technician designation and determines whether a company like ToyTalk would be covered. Much like the privacy policy, the computer technician designation provides little protection, thus Section C proposes an amendment to COPPA necessary to save a child's life. This amendment inserts a duty to report suspected child abuse and neglect for employees and employers. Section D returns to Tiara, and it discusses how our hypothetical interaction would be resolved if such a duty to report existed. Section E provides guidance to companies like ToyTalk that would be impacted by such an amendment. Finally, Section F considers the advantages and disadvantages to the proposal.

A. Hello Barbie Privacy Policy

Hello Barbie's privacy policy is fairly typical. It applies to legal guardians and children[187] and outlines how and what personal information is collected by Hello Barbie. It also provides consumers with a notice and option to accept the terms and conditions as discussed above in Part III.[188] This section identifies specific provisions of Hello Barbie's privacy policy and briefly looks at ToyTalk's data collection policies to determine if any self-imposed duty to report exists.

Hello Barbie's privacy policy includes several sections regarding the specific consumer information that is collected. For example, the policy discusses where the collected information is stored, who has access to such information, and how a guardian can control the information collected. The privacy policy identifies three methods of information collection: active collection, passive collection, and voice recordings. Active collection occurs when the child and guardian configure the doll setup. ToyTalk requires certain personal information about the guardian as well as the child in order to create a Hello Barbie account. Such information includes "parental email and password, [and] [additional information]…such as indicating their child's birthday, what holidays to remember, and other conversation options..."[189] In contrast, passive collection includes data from "Companion Apps or speech processing services being

---

187 *See Hello Barbie/Barbie Hello Dreamhouse Privacy Policy*, TOYTALK, https://www.toytalk.com/hellobarbie/privacy/ (last updated Sept. 9, 2016) (defining children "any child under the age of thirteen. It does not make any statements about children thirteen or older") [hereinafter *Hello Barbie Privacy Policy*].

188 *See infra* contract Part III.

189 *Hello Barbie Privacy Policy*, *supra* note 187.

used." It can also include logistical information in server logs, IP addresses, and the frequency of sessions. Passive data collection is also achieved by "cookies," which are "small data files stored on your hard drive at the request of a website."[190] The final category of data collection is voice recordings. This is the focus of this article and one of the most concerning aspects of Hello Barbie. ToyTalk states that each time a child or user presses Barbie's belt buckle to talk, the company "may capture the voice recordings."[191]

However, to comply with COPPA, the privacy policy states that any "additional personal information" provided to Hello Barbie is deleted once the company becomes of aware of it.[192] Because the privacy policy does not provide a formal definition for personal information, it is unclear exactly what additional information ToyTalk will delete.[193] Each method of information collection provides examples of personal information, but there is no clear guidance on what "additional personal information" means.[194]

---

190 *Id.*

191 *Id.*

192 *See id.*

193 *See id.* Instead, throughout the policy it suggests different types of data included. Specifically, personal information can include "name, email, and telephone number…as well as demographic information;" "device model and name, operating system and version, the browser type, mobile network information, preferred language, time zone, and activity of the Service." Personal information may also include "certain logistical information in server logs, including information about how various features of our service are used and information about the number, frequency and length of each session;" all information collected by cookies; and certain identifiers such as an "Apple IDFA or the Android Advertising ID."

194 Looking at the ToyTalk privacy policy, the definition of personal information seems to follow the definition of personal information from COPPA. COPPA defines personal information as any "individually identifiable information about an individual collected online" such as name, physical address, online credentials such as username and password, phone number, social security number, IP address, geolocation, etc." *See Privacy Policy*, TOYTALK, https://www.toytalk.com/legal/privacy/ (last updated Jan. 11, 2016); 15 U.S.C. § 6501(8) (2016) (defining personal information as "individually identifiable information about an individual collected online, including:
(1) A first and last name;
(2) A home or other physical address including street name and name of a city or town;
(3) Online contact information as defined in this section;
(4) A screen or user name where it functions in the same manner as online contact information, as defined in this section;
(5) A telephone number;
(6) A Social Security number;
(7) A persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier;
(8) A photograph, video, or audio file where such file contains a child's image or voice;

To comply with COPPA, the Hello Barbie privacy policy also states the company's uses for the data collected. Hello Barbie uses parental email and information to ensure proper consent is given.[195] This information is broadly used to provide notice of product updates, promotions and news, to respond to parent/guardian communications, to monitor usage of the app, and to address any general customer service needs.[196] The policy also states that the Hello Barbie complies with COPPA and does not share personal information or voice recordings with third persons except in the following manners: if the user consents to such sharing,[197] to provide potential vendors, consultants, or services necessary information to help maintain the services necessary for Hello Barbie's swift functioning;[198] to provide any information required by law;[199] and

(9) Geolocation information sufficient to identify street name and name of a city or town; or (10) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.").

195 *See Hello Barbie Privacy Policy*, *supra* note 187.

196 *See id.* ("…to provide and maintain the speech processing services and to send you notifications, confirmations, updates, product announcements, security alerts, and support and administrative messages and otherwise facilitate your or your children's use of, and our administration and operation of, the speech processing services; to respond to your communications and requests, provide customer service, notify you about important changes to our speech processing services, Terms of Use, and Privacy Policy or other policies and otherwise contact you about your or your children's use of the speech processing services; to monitor and analyze usage and activities regarding the Site and the Companion Apps; and to provide you with news and information about ToyTalk, The Barbie Products, and products, services, events, activities, offers, and promotions we think will be of interest to you (with your consent where prior consent is required by applicable law) unless you opt out of such use.").

197 *See id.* Sharing information is permissible "when you give us your consent to do so, including if we collect account related information from you and notify you that the information you provide will be shared in a particular manner and you provide such information."

198 *See id.* Sharing information is permissible "with vendors, consultants, and other service providers who need access to such information to carry out their work for us, such as vendors who assist us in providing and maintaining the speech processing services, in developing, testing and improving speech recognition technology and artificial intelligence algorithms or in conducting research and development or who otherwise provide support for the internal operations of the speech processing services (e.g. if we use the Bing Voice Recognition API in connection with the speech processing services, voice recordings and other performance data associated with the speech functionality will be sent to Microsoft.").

199 *See id.* Sharing information is permissible "when we believe in good faith that we are lawfully authorized or required to do so or that doing so is reasonably necessary or appropriate to (a) comply with any law or legal processes or respond to lawful requests or legal authorities, including responding to lawful subpoenas, warrants, or court orders; or (b) protect the rights, property, or safety of ToyTalk, our users, our employees, copyright owners, third parties or the public, to enforce or apply this Privacy Policy, our Terms of Use, or our other policies or agreements.

any information required for the sale, merger, or acquisition of ToyTalk. [200]

Neither Hello Barbie's privacy policy nor ToyTalk's privacy policy provides any requirements similar to a duty to report suspected child abuse or neglect. In fact, both privacy policies expressly state that any additional personal information provided by a minor will be deleted. This disclaimer combined with a guardian's access to such recorded conversations allows ToyTalk to push any monitoring responsibility onto the parent or guardian.

B. The Computer Technician Designation

As described above, Hello Barbie's privacy policy strategically limits any duty ToyTalk may have to notify a parent or guardian about their child's recorded speech. In fact, the Hello Barbie privacy policy makes it so the company may notify the parents or guardians, but it must delete any additional information. Similarly, the Hello Barbie FAQs repeatedly state that it is the responsibility of the parents or guardians to review their child's recorded speech.[201] Any concerning conversations between Hello Barbie and the child can be viewed and handled appropriately by the parent or guardian at any time on the mobile application.[202] Interestingly, the FAQs acknowledge if the company has such a duty to report, it will cooperate "with law enforcement agencies and legal processes as required to so."[203] But does such a duty to report ever exist?

Recall the California duty to report. California and five other states mandate computer technicians to report any suspected child abuse or neglect.[204] Under California law, the computer technician designation includes employees who work in the computer repair or servicing industry, such that the technician may have access to the computer, its memory, and any saved or marked files or Internet searches. This designation also applies to any company that offers "remote computing services" or "electronic communication services."[205] It is clear

---

200 *See id.* Sharing information is permissible "in connection with, or during negotiations of, any merger, sale of company assets, financing or acquisition, or in any other situation where personal information may be disclosed or transferred as one of the business assets of ToyTalk."

201 *See* HELLO BARBIE FAQS, *supra* note 3, at 4.

202 *See id.*

203 *Id.* at 5.

204 MANDATORY REPORTERS OF CHILD ABUSE AND NEGLECT, *supra* note 14, at 2.

205 18 U.S.C. § 2258A (2016); *see Congress Passes New Rules for Child Pornography Reporting by ISPs*, LEXOLOGY (Oct. 22, 2008), http://www.lexology.com/library/detail.aspx?g=f7bc565c-a046-4470-9503-4140e42d29b7 (discussing the PROTECT Our Children Act, "which expands existing child pornography reporting requirements and enhances the government's ability to prosecute producers and traffickers of child pornography.").

from the basic difference in job function that the ToyTalk employees who review the recorded speech are not computer technicians, as these employees are not in the business of computer repair or servicing. Thus for ToyTalk to be covered under this designation, the company must qualify as either a remote computing services or an electronic communication services company. The PROTECT Our Children Act defines these terms. This Act specifically imposes a duty to report on electronic communication service providers and remote computing services, which ToyTalk may be classified under. An electronic communication service means "any service which provides to users thereof the ability to send or receive wire or electronic communications."[206] This broad definition has previously included cable companies, telephone companies, corporate offices, and even libraries. Remote computing services means "provision to the public of computer storage or processing services by means of an electronic communications system."[207] An electronic communications system is "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."[208] Remote computing services include YouTube and a computer bulletin board service.[209]

It seems that ToyTalk and its employees may fall under the electronic communication service provider definition, because ToyTalk receives recorded speech through electronic means.[210] Recent court interpretations of the electronic services definition also suggest that ToyTalk may be categorized under this definition, but there is no definitive answer.[211] This means that such a duty

---

206 18 U.S.C. § 2510(15).

207 *Id.* § 2711(2).

208 *Id.* § 2510(14).

209 *See* Steve Jackson Games, Inc. v. U.S. Secret Service, 816 F. Supp. 432, (W.D. Tex. 1993), *aff'd*, 36 F.3d 457 (5th Cir. 1994); *see* Viacom v. YouTube, 2008 WL 2627388 (S.D.N.Y. 2008).

210 There is some debate if Wi-Fi access points or home users are included under this broad definition. An Arstechnica article provided insight from "Orin Kerr—the legal scholar who wrote the DoJ's electronic search manual, which is linked above as giving Justice's position. And Kerr says it's not so: 'WiFi access points aren't providers of ECS.' There is, he allows, a textual reading on which you could shoehorn the neighborhood cafe into that category, but Kerr says it's 'clearly not what Congress intended.'" Julian Sanchez, *Are You an "Electronic Communication Service Provider"?*, ARSTECHNICA (Feb. 2, 2009), http://arstechnica.com/tech-policy/2009/02/are-you-an-electronic-communication-service-provider/.

211 Courts have generously used this definition to include unexpected entities such as libraries and corporate offices. *See* Steve Jackson 816 F. Supp. at 432; *see* Viacom 2008 WL 2627388.

to report may already exist for ToyTalk in the state of California. But does this duty exist in other states? What if Tiara lived in Virginia? Virginia does not require all persons to report suspected abuse or neglect, nor does the state law include the computer technician designation like in California.[212] If the child is located in a state like Virginia, Tiara's speech recordings will likely go unreported. However, even states like California that impose a broader duty to report, the duty on ToyTalk is questionable at best. In states like Virginia and even Alaska (which has a very narrow computer technician designation), there will likely be no duty to report at all. This is a problem and to eliminate such a harmful gap in the protection of the information of minors, I propose a multifaceted solution below.

C. Proposal to Bridge the Gap

In order to bridge the gap between tort common law and COPPA, I propose an amendment to COPPA. More specifically, I suggest that COPPA include an affirmative duty for companies like ToyTalk to monitor and track suspicious recordings like Tiara's comments about sexual abuse. In addition to the affirmative duty to monitor, COPPA should include a duty to report requirement for computer technicians and service providers. The computer technicians and service providers' definitions can be adopted from the California common law duty to report and modified to extend coverage. The proposed language should be inserted in 15 U.S.C. §6502 directly after subsection (1)(D).[213] It shall state "(2) Duty to Report. Any operator of any website or online service or its employees that has cause to suspect abuse or neglect shall report."[214] Employees shall be defined as:

"a person who works for a company that is in the business of repairing, installing, or otherwise servicing a computer or computer component, including, but not limited to, a computer part, device, memory storage or recording mechanism, auxiliary storage recording or memory capacity, or any other material relating to the operation and maintenance of a computer or computer network system, for a fee. A person interprets personal data, speech recordings, and visual data as a part of his employment duties. Further, an employer who provides an electronic communications service or a remote computing service to the public shall be deemed to comply with this article if that employer com-

---

212 *See* VA. ANN. CODE § 63.2-1509-10 (2016).

213 The previous subsection (2) "When Consent is not Required" shall be relabeled (3). *See* 15 U.S.C. § 6502 (2016).

214 I borrowed language from the North Carolina duty to report law. *See* N.C. GEN. STAT. § 7B-301 (2016).

plies with Section 2258A of Title 18 of the United States Code."[215] Example job titles and roles include computer technician, data analyst, speech recognition scientist, writer, speech scientist.[216]

Cause shall mean knowledge or a reasonable suspicion. Reasonable suspicion

"means that it is objectively reasonable for a person to entertain a suspicion based upon facts that could cause a reasonable person in a like position, drawing, when appropriate, on his or her training and experience, to suspect child abuse or neglect. 'Reasonable suspicion' does not require certainty that child abuse or neglect has occurred nor does it require a specific medical indication of child abuse or neglect; any 'reasonable suspicion' is sufficient."[217]

This amendment to COPPA must also address how to report suspected child abuse or neglect. Because each state has specific reporting requirements in their respective duty to report laws, COPPA should defer to these statutes. These state laws will have the proper reporting requirements and include information necessary regarding what state authorities the employee or company must report the suspected abuse or neglect to. The FTC should be sure to disseminate a press release that summarizes the amendment and refers employers and employees to the Child Welfare Information Gateway's list of State Child Abuse and Neglect Reporting Numbers. This source provides an updated list of each state's reporting information.[218]

D. Returning to Tiara

If this amendment was added to COPPA and the hypothetical situation regarding Tiara and Hello Barbie occurred, her recorded speech would not go

---

215 Language is heavily borrowed from the California penal code definition of computer technician. CAL. PENAL CODE §11165.7 (a)(43)(A)-(B) (2016).

216 Note it is unlikely that there will be conflicts of law issues because the federal law and state laws are not in conflict. Both the proposed amendment to COPPA and state laws are working towards the same goal of preventing child abuse and neglect. Employees and employers that are required to report under the proposed amendment to COPPA must also make sure they comply with the relevant state law. In most scenarios, the employer/employee who is reporting the suspected abuse will be considered a "permissive reporter" and have little obligation under state law. If there are any other state laws that conflict with the proposed amendment to COPPA, it is very likely that COPPA, the federal law, will preempt state law.

217 PENAL §11166(a)(1).

218 *See State Child Abuse and Neglect Reporting Numbers*, CHILD WELFARE INFO. GATEWAY, https://www.childwelfare.gov/organizations/?CWIGFunctionsaction=rols:main.dspROL&rolType=custom&rs_id=5 (last visited Dec. 16, 2016).

unheard. ToyTalk would implement the compliance plan proposed below, creating a code and necessary recording requirements. ToyTalk's code would detect several triggers and require a human employee to review her account and speech. The employee would see that there is a trend in Tiara's communication. Each time she prepares to go to her aunt's house, she becomes upset and nervous. She would tell Barbie that she feels sick and does not want to go. She would also tell Barbie about how her uncle touches her. At this point, the ToyTalk employee must fill out an incident report, saving a copy of the recorded speech, and must contact Tiara's parent/guardian. If Tiara explicitly says "he touches my privates" or similar language that clearly demonstrates child abuse, the ToyTalk employee must immediately report this situation to the proper authorities.

E. How Smart Toy Manufacturers Can Comply

Companies that are operators under COPPA can comply with this amendment in a cost-efficient manner. For example, a company can create software code that searches for certain words and phrases such as "I don't like to be touched" or "daddy touches me." These words and phrases will be considered trigger words and flag the child's individual account. Because speech recordings can be taken out of context, a human employee must review the flagged speech to ensure there is no actual threat of harm. If the speech does not indicate an actual threat, then the employee can remove the flag and the child's profile will be restored to a state that requires no further monitoring. If the speech is unclear and slightly suspicious, the employee can record this instance in some sort of log or incident report and the company may also consider alerting the parents/guardians to such language. Finally, if the speech clearly describes child abuse or neglect, the company must report the suspected abuse to the parents/guardians, and to the proper authorities. The company must also immediately save copies of recorded speech, in case the abuser is the parent/guardian. These copies will be given to the authorities upon report.

It may take some time to create an efficient bank of trigger words and phrases; however, the code will be moderately simple to create. Technology-based companies like ToyTalk will have an advantage because many of their employees can create such codes, so additional costs will be limited. However, there may be additional costs for employee training and education on when the duty to report and the duty to investigate is implicated. These training programs can be based on state law programs that are currently used.[219]

---

[219] *See, e.g.*, *Reporting Suspected Abuse or Neglect of a Child Training*, TEX. DEP'T OF FAM. & PROTECTIVE SERV., https://www.dfps.state.tx.us/training/reporting/ (last visited Nov. 6, 2016) (demonstrating an example of a state issued training program); *see also USC Em-*

F. Advantages and Disadvantages of the Proposed Approach

This section addresses the challenges to the above-mentioned proposal, and considers the advantages and disadvantages. Some may argue that the time and costs of implementing such a tracking program will be too great, and that those costs will negatively impact sales. As previously discussed above, the costs of implementing a new system will be fairly low. Unless ToyTalk decides to hire new employees solely to review flagged profiles, it can utilize the preexisting employees who currently review children's recorded speech. Critics may also argue that this situation is unlikely to occur and to require companies to add safeguards 'just in case' is highly burdensome and inefficient. The likelihood of this situation may be low, but as discussed above, companies need only endure a very small burden to comply with this new portion of COPPA.

Additionally, critics may argue that the new duty to report and investigate leads to less privacy, as it requires employees to examine speech recordings and determine whether they are suspicious. This is not necessarily the case. ToyTalk employees already review recorded speech to improve Barbie's natural language processing capabilities.[220] This proposal only requires the manufacturer to review certain speech that has been marked as suspicious. This approach does not require all recorded speech be examined and analyzed.

Further, there is the Big Brother argument. If ToyTalk discovers recorded speech that suggests there is child abuse or neglect, the company must report it to the proper authorities. This means that the government will become involved and will likely request all of the child's speech recordings. Critics may argue that the government will take advantage of this new duty to report and develop new ways to gain access to and surveillance over children. It is true that the government will become involved if the requested information suggests child abuse, but that is the extent of the government's involvement. Critics should be more concerned with other private companies receiving access to children's personal information and recorded speech. Per the ToyTalk privacy policy, some of the minor's information is already given to third parties.[221]

A final concern is that children may say things to dolls that are exaggerated and sometimes not true. What if the code and the human employee are unable to determine that the child is not being serious? This proposal has a triage-like structure. If there are no signs of abuse or neglect, the flag is removed from the

---

ployee Acknowledgment of Duty to Report Child Abuse, UNIV. OF SO. CAL., https://policy.usc.edu/files/2012/06/USC-Employee-Acknowledgment-on-Child-Abuse.pdf (last visited Nov. 6, 2016).

220 *See* HELLO BARBIE FAQS, *supra* note 3, at 5 ("Conversations…are not monitored in real time, and no person routinely reviews those conversations.").

221 *Hello Barbie Privacy Policy*, *supra* note 187.

child's profile; if there are slightly suspicious recordings, the employee must fill out an incident report and report to the parents; and if there are blatant signs of abuse or neglect, then the employee must report it to the proper authorities. Thus, if there are not explicit statements of child abuse or neglect, the employee should report the suspicious activity to the parents/guardians. The employee should also record this instance, log it in an incident report, and keep the record on file. If there are multiple instances like this, then the employee should reconsider reporting this speech to the proper authorities.

This proposal has many positive implications. The most important is that it has the potential to save a child from a dangerous and unhealthy situation at little cost to companies like ToyTalk. This proposal is not intended to burden companies like ToyTalk with more procedural requirements and costs. This proposal aims to use these new technologies to help prevent future harm to children. Developmental psychologists promote imaginary play with dolls or toys because it helps create many behavioral benefits when children pay with dolls.[222] Children form necessary life skills including the ability to make and foster relationships.[223] Children also form strong bonds with their toys and often confide in them. Hello Barbie has the potential to be that doll and the public can use this to its advantage to prevent or stop child abuse and neglect.

CONCLUSION

With smart toys rapidly propagating, privacy concerns will continue to grow. This article identifies critical privacy concerns stemming from the growing adoption of smart toys by an increasingly younger generation eager to share sensitive personal information, and it proposes a solution to balancing the right to privacy vis-à-vis the duty to report. More specifically, the proposed amendment to COPPA makes companies such as ToyTalk mandatory reporters

---

[222] In fact, the psychological benefits of playing with inanimate objects, such as dolls, are well known, "it stimulates tolerance, emotional intelligence and empathy, develops richness of metaphoric thinking and expression, the growth of imagination and creativity." *See* Jasna Gržinić et al., *Child and Psychological Aspects of a Doll*, 5 METODIČKI OBZORI 9, 45–46 (2010).

[223] *See* Lauren Walker, *Hello Barbie, Your Child's Chattiest and Riskiest Christmas Present*, NEWSWEEK (Dec. 12, 2015), http://www.newsweek.com/2015/12/25/hello-barbie-your-childs-chattiest-and-riskiest-christmas-present-404897.html ("We learn a lot about a child's anger and their family life based on how they play and what is talked about during child's play," says Dr. Judith Fiona Joseph, a child and adolescent psychiatrist with a practice in New York City. "You can learn a lot about what your child observes." Sexual or violent movie scenes, for instance, may make their way into play sessions. "Parents must be very prepared for what they may learn about their children through the recordings," she says.").

if there is a reasonable suspicion of child neglect and abuse. Such a proposal is reasonable since the company already reviews the recorded speech to enhance and modify its product. In addition to the proposed amendment, this article presents a practical method in which companies can comply. This solution aims to protect children who are in danger without shackling smart toy companies with heavy burdens and expenses. Hello Barbie is just the beginning. This article aims to incite thought and action to prevent similar instances from occurring.