MANDATED ETHICAL HACKING—A REPACKAGED SOLUTION

Cite as: Corinne Moini, *Mandated Ethical Hacking—a Repackaged Solution,* 23 Rich. J.L. & Tech. Ann. Survey (2017), http://jolt.richmond.edu/volume23_annualsurvey_moini/.

By: Corinne Moini*

I. INTRODUCTION

[1] Since the early 2000s, the consumer market for artificial intelligence ("AI") has boomed.[1] Each year, tech giants like Apple and Samsung have released a new smart device[2] in the form of a phone, television, DVD player, or household appliance. Within the last five years, the target market for these smart devices has expanded to include

* J.D. Candidate 2017, University of Richmond School of Law. B.A., 2013, Virginia Tech University. B.S., 2014, Virginia Tech University. The author would like to thank the editors and staff of the Richmond Journal of Law & Technology for their efforts in editing this article.

[1] *See* Daniel Fagella, *Valuing the Artificial Intelligence Market, Graphs and Predictions for 2016 and Beyond*, TECH EMERGENCE, https://www.techemergence.com/valuing-the-artificial-intelligence-market-2016-and-beyond/, https://perma.cc/UAX2-MMAV (last updated Mar. 7 2016). "Artificial Intelligence is the simulation of human intelligence processes by machines, especially computer systems." Margaret Rouse, *AI (Artificial Intelligence)*, TECH TARGET, http://searchcio.techtarget.com/definition/AI, https://perma.cc/M4SG-6FCH (last visited Apr. 1, 2017).

[2] Smart objects "must be able to sense and interact with their immediate environment, and communicate with devices or humans." *See* Corinne Moini, Comment, *Protecting Privacy in the Era of Smart Toys, Does Hello Barbie have a Duty to Report?*, 25 C.U.J.T. (forthcoming May 2017). These objects "use WiFi, Bluetooth, or mobile apps, and offer "smart" features such as cameras, microphones, and sensors that can record and respond to…interactions." *Digital Toy Poses Possible "Spy Toys" Privacy Violations*, FOX 43 (Dec. 9, 2016, 4:21PM) http://fox43.com/2016/12/09/digital-toys-pose-possible-spy-toys-privacy-violations/, https://perma.cc/647M-ZDE5 [hereinafter *Digital Toy*].

children.[3] Toy manufacturers such as Mattel and VTech have started making toys that utilize wireless technologies such as Wi-Fi and Bluetooth.[4] Two of the most notable and controversial smart toys to hit the market are Hello Barbie, produced by Mattel and ToyTalk, and My Friend Cayla, produced by Genesis Toys and Nuance Communications. These dolls were projected to produce substantial revenues of over two billion dollars.[5] However, both toys have experienced rather disappointing returns, largely due to negative product reviews and more relevantly major privacy vulnerabilities exposed by data hacks.[6] More specifically, both Hello Barbie and My Friend Cayla have received public backlash from privacy activists,[7] concerned parents groups,[8] and even the German Government.[9] These smart toys were labeled as "creepy,"[10] "insecure,"[11]

[3] *See Artificial Intelligence (Chipsets) Market Worth 16.06 Billion USD by 2022*, MKTS AND MKTS, http://www.marketsandmarkets.com/PressReleases/artificial-intelligence.asp%20.asp, https://perma.cc/7Z7K-8S8M (last visited Mar. 20, 2017).

[4] *See* Yewande Ogunkoya, *Internet-Connected Toys Are Spying on Kids, Threatening Their Privacy and Security*, CTR. FOR DIGITAL DEMOCRACY (Dec. 6, 2016), https://www.democraticmedia.org/filing/internet-connected-toys-are-spying-kids-threatening-their-privacy-and-security, https://perma.cc/P7CB-YWT3.

[5] *See* John Kell, *Mattel's Barbie Sales Down for a Third Consecutive Year*, FORTUNE (Jan. 30, 2015), http://fortune.com/2015/01/30/mattels-barbie-sales-drop-third-year/, https://perma.cc/96AD-SVVE; *Digital Toy*, *supra* note 2.

[6] The phrase "data hack" and "data breach" will be interchangeably throughout this article. *See* John Kell, *supra* note 5.

[7] *See* Lauren Walker, *Hello Barbie, Your Child's Chattiest and Riskiest Christmas Present*, NEWSWEEK, (Dec. 15, 2015, 9:34 AM) http://www.newsweek.com/2015/12/25/hello-barbie-your-childs-chattiest-and-riskiest-christmas-present-404897.html, https://perma.cc/2Z2L-K2XT.

[8] *See* Sophie Harris, *"Hell No Barbie" Campaign Targets Hello Barbie Concerns*, CBC NEWS (Oct. 29, 2015 5:00AM), http://www.cbc.ca/news/business/hello-barbie-1.3292361, https://perma.cc/F9RG-6W9A; *see* Martha Neil, *Mom Sues Mattel, Saying "Hello Barbie" Doll Violates Privacy*, ABA J. (Dec. 9, 2015 11:25 AM) http://www.abajournal.com/news/article/hello_barbie_violates_privacy_of_doll_owners_playmates_moms_say_in_lawsuit/, https://perma.cc/8S79-QXVM.

[9] *See* Soraya Sarhaddi Nelson, *Germany Bans 'My Friend Cayla' Doll Over Spying Concerns*, NPR (Feb. 20, 2017 4:40PM),

and an "espionage device,"[12] as each device was released to the general public. Despite these smart toys' lack of success, toy manufacturers continue to produce and release new smart toys of a similar structure and function. Some examples of the continued production of these smart toys include the releases of a revamped Teddy Ruxpin and Cloud Teddy.[13]

[2] The critical question is whether the claims against these toys have merit, or more succinctly: do these smart toys deserve such a bad rap? Are these dolls as creepy and insecure as its opponents suggest? Are the threats of data hacks and breaches for children's smart toys real? While the "creepiness" or "insecurity" of these toys may be up for debate, their vulnerability to data breaches is a very real issue.

[3] Several smart toys including Hello Barbie, My Friend Cayla, and the VTech tablet have been subject to known data hacks in 2015.[14]

---

http://www.npr.org/2017/02/20/516292295/germany-bans-my-friend-cayla-doll-over-spying-concerns, https://perma.cc/D8D5-N4KP.

[10] *See* Mark P. Mills, *Creepy Barbie? Brace Yourself for the Internet of Toys*, FORBES (Dec. 22, 2015 6:17PM), https://www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/markpmills/2015/12/22/hello-barbie-made-the-naughty-list-brace-yourself-for-the-internet-of-toys/&refURL=https://www.google.com/&referrer=https://www.google.com/, https://perma.cc/9NVP-6K6K.

[11] *See* Laura Hautala, *Hello Barbie: She's Just Insecure*, CNET (Dec. 4, 2015 3:00AM), https://www.cnet.com/news/hello-headaches-barbie-of-the-internet-age-has-even-more-security-flaws/, https://perma.cc/5D9H-MYPC.

[12] *See* Andrea Thomas, *Germany Issues Kill Order for a Domestic Spy- Cayla the Toy Doll*, WALL ST. J. (April 13, 2017 11:52AM), https://www.wsj.com/articles/germany-issues-kill-order-for-a-domestic-spycayla-the-toy-doll-1492098755, https://perma.cc/4ZSN-L8YK.

[13] *See* Parija Kavilanz, *Ionic '80s Toy Bear Teddy Ruxpin is Back*, CNN TECH (Sept. 30, 2016 1:49PM), http://money.cnn.com/2016/09/30/technology/teddy-ruxpin-toy-bear/, https://perma.cc/6C7G-EJTV.

[14] *See* David Moye, *Talking Doll Cayla Hacked to Spew Filthy Things (Update)*, HUFF. POST (Feb. 9, 2015 4:10PM), http://www.huffingtonpost.com/2015/02/09/my-friend-cayla-hacked_n_6647046.html, https://perma.cc/S95Y-KNB8; *see* Jared Newman, *Internet- Connected Hello Barbie Doll Can Be Hacked*, PC WORLD (Dec. 7, 2015

Additional toys, such as Cloud Teddy, have been reported hacked already in 2017.[15] However, it is important to note the cyber-security attacks against Hello Barbie, My Friend Cayla, and VTech differ from the attack against Cloud Teddy because Cloud Teddy was hacked for its information and potential ransom profits. These other toys were hacked to demonstrate security vulnerabilities. In fact, many recent hacks against smart toys are done to prove a point; the hacker is not interested in stealing information or receiving ransom money. The point is that these smart toys are insecure, breach-able pieces of hardware, and that can serve as gold mines of information for other hackers. By infiltrating the systems of smart toys like these, hackers can potentially steal information about both the minor as well as their guardians. This article will focus on this type of hacking—hacking "ethical hacking" or merely to prove a point—and its utilization in the exposing of smart toys' potential for data breaches.

[4] Hacking to prove a point or to expose technological vulnerabilities has been around since the 1960s, but it has been labeled and packaged differently as "white hacking" or "ethical hacking."[16] This article suggests that smart toy manufacturers, such as Mattel and VTech, should be subject to required vulnerability testing which utilizes ethical hacking under the Consumer Product Safety Improvement Act ("CPSIA"). More specifically, this article proposes to amend the Toy Safety Standard, ASTMF- 963-11, to include smart toys connected to the internet. The CPSIA and Consumer Product Safety Commission ("CPSC") impose safety testing on all toys intended for use by children of twelve years of

9:17AM), http://www.pcworld.com/article/3012220/security/internet-connected-hello-barbie-doll-can-be-hacked.html, https://perma.cc/WB46-E5PS.

[15] *See* Rod Chester, *Millions of Recorded Messages Between Parents and Children Targeted in Teddy Bear Toy Hack*, NEWS.COM.AU (Feb. 28, 2017 10:40AM), http://www.news.com.au/technology/online/security/millions-of-recorded-messages-between-parents-and-children-targeted-in-teddy-bear-toy-hack/news-story/d8a4f09e975a6f83f7bd24ec22f40dc5, https://perma.cc/7269-PC47.

[16] Ethical hacking "at its core [] involves ethical principles that would prohibit taking advantage of a potential target's lack of security….Ethical hackers aim to create a more secure Internet." Trevor A. Thompson, Comment: *Terrorizing the Technological Neighborhood Watch: The Alienation and Deterrence of the "White Hats" Under CFAA*, 36 FLA. ST. U.L. REV. 537, 554 (2009).

age or younger.[17] This article will explore the proposed safety testing in the context of the smart toy My Friend Cayla and Hello Barbie. This article is cognizant of how fast-paced the technology industry and thus, does not suggest a specific time period, rather it suggests what must be done prior to the release of product.

[5] The paper proceeds as follows: Section IIA will provide brief history of data hacks and recent trends for infiltrating various systems. Section IIB will further detail the history of ethical hacking, (once referred to as white hacking.) Section IIC will provide a brief description of smart toys and notable data hacks with smart toys. Additionally, Section IIC will look at existing standards that companies have for testing security vulnerability. Section III will briefly describe relevant privacy and security breach laws, as well as briefly explaining the CPSIA. Section IV will propose an amendment to the existing ASTMF-963-11 toy standard and a sample compliance plan for companies. Section IV will also explore advantages and disadvantages of this proposal. Section V will provide a brief conclusion, calling for the reconsideration of the utilization of ethical hacking in the limited scope of children's smart toys.

II. SMART TOYS AND DATA HACKS

[6] According to the Identity Theft Resource Center, "U.S. companies and government agencies suffered a record 1,093 data breaches last year, a 40 percent increase from 2015."[18] Additionally, a 2016 study suggests the chances of being hacked are about one in three, for every individual that

[17] *See* CONSUMER PRODUCT SAFETY IMPROVEMENT ACT OF 2008, 110 Pub. L. No. 314, 122 Stat. 3016 (2008).

[18] Olga Kharif, *2016 Was a Record Year for Data Breaches*, BLOOMBERG (Jan. 19, 2017, 7:00AM), https://www.bloomberg.com/news/articles/2017-01-19/data-breaches-hit-record-in-2016-as-dnc-wendy-s-co-hacked, https://perma.cc/U45V-QJGZ; *see also* Andrew Braunstein, *Standing Up for their Data: Recognizing the True Nature of Injuries in Data Breach Claims to Afford Plaintiffs Article III Standing*, 24 J.L. & POL'Y 93, 100 (2015) ("Since 2005, more than 534 million personal records have been lost as a result of data breaches. In 2014 alone there were 579 separate data breaches and experts predict this number will only rise 'as consumers become more dependent on Internet-connected devices.' The actual number of breaches is likely even higher because security experts generally agree that most breaches are never reported to the public.")

accesses the internet with a smart device.[19] What was once the remote possibility of a data hack has shifted into the realm of becoming a legitimate probability. Recent articles by major news outlets such as Forbes and the Atlantic warn readers of *when* the hack will occur not *if* it will.[20] Despite growing public knowledge and a continuous influx of new security measures, the rate of cybersecurity attacks continues to grow as hackers crave new information. Typically, hackers seek financial information such as credit card numbers and personal identifiable information ("PII") such as "names, addresses, email addresses, and phone numbers, Social Security numbers, bank account numbers, [passport and license numbers], or medical records."[21] On some occasions, the data hacks extended even further into an individual's privacy, with the hackers seizing photographs and even stored recorded speech.[22]

[7] Unsurprisingly, the transition to paperless documentation process is seen as a correlating factor to the rise in cybersecurity attacks and data hacks.[23] As more companies operate and store files online, the opportunity for hackers to infiltrate the system grows. Potential victims range from the healthcare industry to financial companies, retailers, professional companies such as law firms and accounting firms, individuals, and even educational institutions.[24] The remainder of this section will provide a

[19] *See* Ben Taylor, *Why There is a 1 in 3 Chance You'll Get Hacked in 2016*, BEST VPN, (Mar. 2, 2016), https://www.bestvpn.com/blog/43225/get-hacked-one-in-three/, https://perma.cc/9AVW-WPR9.

[20] *See* Andrew McGill, *The Inevitability of Being Hacked*, ATLANTIC, (Oct. 28, 2016), https://www.theatlantic.com/technology/archive/2016/10/we-built-a-fake-web-toaster-and-it-was-hacked-in-an-hour/505571/, https://perma.cc/NUF3-JSYT; *see* Samantha Drake, *Chances are Your Startup is Going to Get Hacked—Here's What to Do*, FORBES (Feb. 3, 2017 5:01PM), https://www.forbes.com/sites/samanthadrake1/2017/02/03/chances-are-your-startup-is-going-to-get-hacked-heres-what-to-do/#4ab11990ce25, https://perma.cc/8EU6-TYZH.

[21] *See* Andrew Braunstein, *supra* note 18, at 101.

[22] *See id.*

[23] *See id.* at 103.

[24] *See id.* at 102–03.

brief history of hacking and the most common forms of hacking today as well as a brief introduction of smart toys and recent smart toy hacks.

A. The History of Hacking

[8] The act of hacking can be traced back to the 1870s with the British government hacking phone systems.[25] Contemporary hacking, however, is more closely linked to the style of hacking that arose in the 1960s, where universities, such Massachusetts Institute of Technology, encouraged their researchers to hack.[26] During this time, universities that focused on artificial intelligence defined a hacker as "a person with a mastery of computers who could push programs beyond what they were designed to do."[27] In the 1970s and 1980s, hacking began to develop a negative connotation as persons like John Draper and the Milwaukee-based 414s used hacking for illegal purposes.[28] Additionally, the act of "phreaking," manipulating telecommunication systems, gained publicity as a form of hacking.[29] As a result, the Secret Service began to enforce computer fraud

[25] *See* Robert Trigaux, *A History of Hacking*, ST. PETERSBURG ONLINE, http://www.sptimes.com/Hackers/history.hacking.html, v= https://perma.cc/BF5Y-XQHW (last visited Apr. 20, 2017) ("However, the power of hacking was not fully recognized until the invention of the transistor in the 1940s.") be interesting to know specifically how they were doing it in an explanatory.

[26] See *id.*

[27] *Id.*

[28] *See id.* ("John Draper makes a long-distance call for free by blowing a precise tone into a telephone that tells the phone system to open a line. Draper discovered the whistle as a give-away in a box of children's cereal. Draper, who later earns the handle "Captain Crunch," is arrested repeatedly for phone tampering throughout the 1970s. In one of the first arrests of hackers, the FBI busts the Milwaukee-based 414s (named after the local area code) after members are accused of 60 computer break-ins ranging from Memorial Sloan-Kettering Cancer Center to Los Alamos National Laboratory.").

[29] *See* Mike James, *A History of Ethical Hacking*, STAYSAFEONLINE.ORG (Aug. 29, 2016 7:19AM), https://staysafeonline.org/blog/a-history-of-ethical-hacking, https://perma.cc/2ANS-9F4D.

under the Comprehensive Crime Control Act and U.S. legislators created the Computer Fraud and Abuse Act.[30]

[9] Today, hacking is seen as a malicious act to illegally obtain proprietary information or to disrupt systems and operations.[31] Hackers, "use programs to log keystrokes, hack passwords, infect systems, create bots (i.e., computers used to send spam or commit distributed denial of service attacks), store illicit material, and steal data."[32] It can be done, secretly or publicly, for a variety of reasons.[33] While financial gain is an obvious motivation for hacking, some believe that hackers largely hack not for the monetary benefits, but "for the thrill of the chase, or as a publicity stunt or out of intellectual curiosity."[34] Additionally, modern hacking may also be influenced by the hacker's politics or personal beliefs. Hackers falling into this category self-describe themselves as "hactivists."[35] For example, the hacking coalition that labels itself as 'Anonymous' is a well-known hactivist group, which has taken credit for the hacks of many companies and government agencies.[36]

---

[30] *See id.*

[31] The ten most common ways are: distributed denial of service attack, remote code execution attacks, cross site request forgery attacks, symlinking, social engineering attacks, DNS cache poisoning, clickjacking attacks, broken authentication and session management attacks, cross site scripting attacks, and injection attacks. *See* Shritam Bhowmick, *10 Most Popular Ways Hackers Hack Your Website*, DEFENCELY, http://defencely.com/blog/tag/types-of-hacking/, https://perma.cc/R4HY-73HJ (last visited Apr. 20, 2017).

[32] Sarah Pearce, *To Hack Back, Or Not To Hack Back, That Is The Question*, LAW360 (Oct. 30, 2014 10:37AM), https://www.law360.com/articles/591476/to-hack-back-or-not-to-hack-back-that-is-the-question, https://perma.cc/3H5Q-65PH.

[33] *Id.*

[34] *Id.*

[35] *Id*

[36] *Id.*

B. A Brief History of Ethical Hacking

[10] Ethical hacking in its simplest form is hacking to create a more secure network by exposing potential vulnerabilities.[37] The hack itself searches for weaknesses and vulnerabilities so that they can be remedied and not taken advantage of by another hacker.[38] The 1960s style of hacking described in Section IIA was one of the first examples of "ethical hacking"—a valuable skill that experts aimed to master.[39] As a result, many consider the history of modern hacking to incorporate the history of ethical hacking.[40] Three out of the four smart toy hacks discussed below in Section IIC are examples of ethical hacking.[41]

[11] In the 1970s, when phreaking became a widespread issue,[42] both the U.S. government and private companies utilized what is now known as ethical hacking.[43] They hired experts to find, report, and in some cases cure any system weaknesses before a third party could exploit them.[44] These experts were called "tiger teams" by the U.S. government.[45]

[37] *See* Trevor A. Thompson, *supra* note 16, at 554.

[38] *Id*.

[39] *See* Mike James, *supra* note 29.

[40] *See id.*

[41] *See infra* Part IIC.

[42] *See* Mike James, *supra* note 29 ("Phreaking refers to the practice of manipulating telecommunications systems. Phreakers began to understand the nature of telephone networks.").

[43] *See id.*

[44] *See id.*

[45] *See* Mike James, *supra* note 29.

[12] In the 1980s and 1990s modern hackers, or hackers with mal-intent, began to materialize.[46] By that time, the term hacking had become associated with illegal criminal activity.[47] Such hackers found that hacking to steal proprietary information could be a lucrative business.[48] Hacking quickly became national news, largely as the result of high-profile hacks, such as Southwestern Bell hack.[49] These hackers, (thieves of proprietary information) eventually obtained the name "black hat hackers."[50] Conversely, what we now know as ethical hackers were given the nickname "white hat hackers."[51] The actual phrase "ethical hacking" was not coined until 1995, by John Patrick, the Vice President of IBM.[52] He suggested that ethical hacking was "the goal of the majority of hackers, but the current media perception is that hackers are criminals."[53]

[14] Due to the growing skill-level and persistence of black hat hackers, the counter-defense of utilizing ethical hacking or white hat hackers is a

[46] *See* Daniel Bukszpan, *6 Notorious Hackers and their Second Careers*, FORTUNE, Mar. 18, 2015, http://fortune.com/2015/03/18/famous-hackers-jobs/, https://perma.cc/78KG-D6LS (discussing famous hackers from the 1980s and 1990s like Robert Tappan Morris, Kevin Poulsen, and Kevin Mitnick).

[47] *See, e.g.* Rich Hardy, *Hollywood and Hacking: The 1980s - kid hackers, nerds and Richard Pryor*, News Atlas (Oct. 9, 2016), http://newatlas.com/history-hollywood-hacking-1980s/45482/, https://perma.cc/NG4U-97R6 (discussing how Hollywood is accredited with hackings bad rap).

[48] *See id.*

[49] *See* Daniel Bukszpan, *supra* note 46.

[50] *See* Sarah Pearce, *supra* note 32.

[51] *See* Trevor A. Thompson, *supra* note 35 at 555–56.

[52] *Id.*

[53] *See* Mike James, *supra* note 29 ("Some of the most skilled and successful ethical hackers started as black hat hackers. For example, Kevin Poulsen, who is now a respected journalist, was actually put in prison for hacking the telephone line of a radio station contest, allowing him to win a Porsche 944 S2. Since his release, he has used his skills to uncover illicit activities on the internet.").

common response of many cybersecurity firms.[54] Today, there are even specific training programs and certifications to become a "Certified Ethical Hacker."[55] Modern ethical hacking or white hat hacking "involves using the same techniques that black hat hackers use in order to break down cyber defenses. The difference is that when a white hat hacker has compromised those defenses they inform the business of how they managed to do it so that the vulnerability can be fixed."[56]

C. Smart Toys[57]

[15] "Smart toys" as used in this article, means toys with the ability to connect to the internet to gather information and interact with its user. These toys fall under a broader category of "intelligent" or "smart" 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").[58] The IoT is a rapidly growing "network of physical devices (or 'things')" which are capable of sensing and collecting data about their environment, and transmit that data via the Internet to an online system, such as a cloud.[59] 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.[60]

---

[54] *See id.*

[55] *See id.*

[56] *Id.*

[57] This section has been excerpted from a previous work: Corinne Moini, *supra* note 2.

[58] *See* Antigone Peyton, Article: *A Litigators Guide to the Internet of Things*, 22 RICH. J. L. & TECH. 9, 9 (2016).

[59] *See id.*

[60] *See id.* at 11.

[16] To qualify as a smart device, these objects must be able to sense and interact with their immediate environment, and communicate with devices or humans.[61] Many of these devices are equipped with sensors[62] and can record sensor signals (e.g., human conversation), later transmitting the recorded data to other devices or external systems via the Internet.[63] Computer scientists are actively working to develop new methods and technologies to automatically process, categorize, and understand massive amounts of data that is being collected by these devices.[64] A relatively new branch of AI research, called Machine Learning ("ML"), focuses on developing computer algorithms, which allow machines to process and transform vast amount of raw data collected by IoT devices into meaningful, actionable information, which can be used by humans.[65] These ML technologies have made the vast amount of information collected by IoT devices into a highly sought after commodity, inadvertently incentivizing hacking.[66]

[17] An example of a toy or "smart toy" that falls into the broader category of "smart object" is Hello Barbie. Hello Barbie is considered the

[61] *See id.* at 12. (possible explanation of what an example of "sense and interact" would be)

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

[63] *See* Antigone Peyton, *supra* note 58 at 12.

[64] *See When IoT Meets Artificial Intelligence*, WAYLAY.IO, http://www.waylay.io/blog-iot-meets-artificial-intelligence.html, https://perma.cc/8SZS-7U96 (last visited Mar. 13, 2017).

[65] *See* Mark Jaffe, *IOT Won't Work Without Artificial Intelligence*, WIRED, https://www.wired.com/insights/2014/11/iot-wont-work-without-artificial-intelligence/, https://perma.cc/ZG7Q-H7GH (last visited Dec. 11, 2016).

[66] "However, the data by themselves do not provide value unless we can turn them into actionable, contextualized information. Big data and data visualization techniques allow us to gain new insights by batch-processing and off-line analysis. 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." *Id.*

first of its kind. She is the first wholly interactive doll.[67] Hello Barbie leverages AI technologies, such as her natural language processing, to deliver a life-like interactive experience to its human subject.[68] AI is a subfield of computer science[69] that strives to create machines with human-like cognitive capabilities.[70] More specifically, AI seeks 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 manner similar to how humans operate.[71] Many of the common devices owned by Americans, such as home appliances, cellphones, TVs, and online music radios like Pandora and Spotify, are increasingly incorporating AI technologies.[72]

[18] In its most simplistic view, Hello Barbie is similar to Siri or Cortana,[73] but the technology is located in a doll and accessed almost entirely children. Hello Barbie listens to what you or your child says and

[67] *See* Chip Chick, *Hello Barbie is World's First Interactive Barbie Doll*, YOUTUBE (Feb. 15, 2015), https://www.youtube.com/watch?v=RJMvmVCwoNM, https://perma.cc/M2BD-U24T.

[68] *See id.*

[69] *See* STUART JONATHAN RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH 18 (3rd 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, https://perma.cc/98MZ-FM52.

[70] *See* Istvan S.N. Berkeley, *What is Artificial Intelligence?*, The University of Louisiana at Lafayette, http://www.ucs.louisiana.edu/~isb9112/dept/phil341/wisai/WhatisAI.html, https://perma.cc/87WM-8AKT (last visited Mar. 30, 2017).

[71] *See* Kris Hammond, *supra* note 69.

[72] *See* Jordan Novet, *Google, Spotify, & Pandora Bet a Computer Could Generate a Better Playlist than You Can*, VENTURE BEAT (Nov. 11, 2014 8:30AM), https://venturebeat.com/2014/11/11/deep-learning-music-streaming/, https://perma.cc/SRC9-83SW.

[73] The intelligent personal assistants featured on Apple and Windows cell phones, respectively.

then uses "breath to bytes"[74] to encode that audio, process the data, 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.[75] These recorded statements are then sent to ToyTalk[76] to generate a response from Barbie, and saved in an online data storage cloud.[77] The responses are stored to help create a more "tailored response…[so it] almost seems like 'she's alive.'"[78] 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.[79] If a parent

[74] JOHN FRANK WEAVER, ROBOTS ARE PEOPLE TOO: HOW SIRI, GOOGLE CAR, AND ARTIFICIAL INTELLIGENCE WILL FORCE US TO CHANGE OUR LAWS 7 (2014) ("translating your words into action") [hereinafter ROBOTS ARE PEOPLE TOO].

[75] HELLO BARBIE MESSAGING/ Q&A, at 3 http://hellobarbiefaq.mattel.com/wp-content/uploads/2015/12/hellobarbie-faq-v3.pdf, https://perma.cc/Z6FL-KN8Z (last visited Mar. 30, 2017) [hereinafter HELLO BARBIE FAQS].

[76] ToyTalk is an entertainment and technology company, that partnered with Mattel to create Hello Barbie. ToyTalk developed the speech recognition and progressive learning technologies for Hello Barbie. *See id.*

[77] Frank Lin, Comment: *Siri, Can You Keep a Secret? A Balanced Approach to Fourth Amendment Principles and Location Data*, 92 OR. L. REV. 193, 196 (2013). 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 amount of consumers projected to use this toy. It also makes it easier to create big data and analyze the children's responses.

[78] 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. 1, 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, https://perma.cc/NT53-2J6M [hereinafter *The Dark Side of Buying your Children Smart Toys*].

[79] *See id.*

or guardian is unhappy with the recorded content, they are able to delete it off the application.[80]

[19] Since the release of Hello Barbie, similar interactive toys have entered the market. For instance, the ionic talking bear Teddy Ruxpin is being revamped and released.[81] The toy is not fully interactive, like Hello Barbie, but contains "a motorized mouth…LCD eyes that show 40 animated expressions synched to the stories."[82] The talking bear also contains an internal hard drive including ten prerecorded stories and the ability to download more.[83] Additionally, Disney Consumer Products and Interactive Media Labs created an interactive Miss Piggy Facebook page, which allows you to Facebook message with the famous Pig.[84] Miss Piggy's interactive Facebook page takes the old AOL Instant Messenger feature of "Smarter Child" to a new level.[85] The fictional Facebook page is powered by Imperson, a company that creates conversational bots, which are robots that are capable of simulating conversations with persons.[86]

---

[80] *See id.*

[81] *See* Parija Kavilanz, *supra* note 13.

[82] *Id.*

[83] *See id.*

[84] *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/, https://perma.cc/9QWW-A2Z5.

[85] *See* Ashwin Rodrigues, *A History of SmarterChild*, VICE: MOTHERBOARD (Mar. 16, 2016, 6:00 AM) http://motherboard.vice.com/read/a-history-of-smarterchild, https://perma.cc/7LNX-B7HF. "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."

[86] Conversational bots are 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, 2:11PM), http://www.bizjournals.com/losangeles/news/2016/02/03/miss-piggy-talks-to-fans-thanks-to-imperson-s-chat.html, https://perma.cc/6H3D-3WXM; *see also* IMPERSON, http://imperson.com/, https://perma.cc/75YC-HV2J (last visited Mar. 8, 2017).

i. Notable Known Smart Toy Data Hacks

[20] Prior to 2015, hackers generally did not target toy manufacturers. Hackers focused on targeting large organizations and institutions, rather than pre-programmed toys and individuals. However, as toy manufacturers like VTech and Mattel began to create internet connected toys, or "smart toys," the hacking landscape began to change. This section provides descriptions of notable cyber-security attacks on smart toys. These hacks were highly publicized and predictably, they significantly contributed to the poor reviews of the products involved.

1. VTech

[21] VTech Holdings is digital toy manufacturer that creates electronic learning devices for children.[87] In November 2015, VTech Holdings experienced a major data hack.[88] The toy company's "Learning Lodge app store customer database, the PlanetVTech and V.Smile Link websites, and Kid Connect servers,"[89] were hacked by an unknown individual. The hacker gained access to the database of addresses, names, birth dates, gender, etc. for over 5 million accounts worldwide.[90] In fact, he was able to expose personal information of "6.4 million children and 4.8 million adults," in only a few hours.[91] The hacker explained that he was able to hack the system using an older hacking technique, (an SQL injection on

[87] *See id.*

[88] *See The Dark Side of Buying your Children Smart Toys*, *supra* note 78.

[89] *FAQ about Cyber Attack on VTech Learning Lodge*, VTECH, https://www.vtech.com/en/press_release/2016/faq-about-cyber-attack-on-vtech-learning-lodge/#9, https://perma.cc/N8QP-SDBE (last updated Dec. 16, 2016) [hereinafter *VTech Press Release*].

[90] *See id.*

[91] Thomas Fox-Brewster, *More Trouble For VTech -- Kids Tablet Is 'Easy' To Hack*, FORBES (Dec. 2, 2015 3:05PM), https://www.forbes.com/sites/thomasbrewster/2015/12/02/vtech-innotab-tablet-easy-to-steal-kids-data/#680c6f0a2863, https://perma.cc/NQS2-J377.

VTech's Flash plugin and login box,) which allowed him to get maximum access to the server.[92] The hacker explained his motivation to a Motherboard journalist, was "to expose the company's inadequate security measures."[93] It took VTech two weeks to even realize they had been hacked.[94]

[22] After the hack occurred, security expert Ken Munro was also able to hack VTech servers.[95] Munro suggested that the hack was rather easy to conduct because the weaknesses of the tablet processor had been known for over two years.[96] In fact, he stated that the "problem lies in the processor within the tablet, the Rockchip RK3168, which allowed anyone with access to the device to easily pilfer data from memory using a freely-available tool called 'rkflashtool.'"[97] Munro suggests that VTech requires a major security update.[98] The company's website and mobile application were not protected by web encryption, leading some to question whether VTech even has a data security team.[99] Since the VTech hack, the company has "reviewed [its] security protocols for Kid Connect and implemented additional measures to protect data transmitted and stored via that service. [It has also] deleted all Kid Connect bulletin board contents and unsent messages before [it] restarted the service."[100] Whether

[92] *See* Lorenzo Franceschi-Bicchierai, *VTech Hacker Explains Why He Hacked the Toy Company*, MOTHERBOARD (Dec. 2, 2015), http://motherboard.vice.com/read/vtech-hacker-explains-why-he-hacked-the-toy-company, https://perma.cc/7MQM-X7DR.

[93] *Id.*

[94] *See id.*

[95] *See* Thomas Fox-Brewster, *supra* note 91.

[96] *See id.*

[97] *Id.*

[98] *See id.*

[99] *See id.*

[100] *VTech Press Release*, *supra* note 89.

these measures have served to effectively combat future hacks of this nature remains to be seen.

2. Hello Barbie

[23] Mattel and ToyTalk partnered to produces the Hello Barbie doll. In November 2015, (the same month as the V-Tech attack,) Hello Barbie experienced a similar hack as V-Tech. A security researcher, named Matt Jakubowski, believed that the doll was "susceptible to being hacked and could compromise its owners' privacy," much like the VTech devices.[101] Jakubowski was able to access the "toy's system to access users' system information, Wi-Fi network names, internal MAC addresses, account IDs and MP3 files...He added that he would be able to use this data to find someone's house and personal information, and could access their home network and listen to everything Barbie records."[102] Jakubowski told NBC News that it was only a matter of time until hackers could replace the servers completely and do anything they want.[103] After this hack became public, a series of articles were released regarding Barbie's vulnerabilities.[104] Security research companies such as Bluebox and Somerset Recon, highlighted additional vulnerabilities of the doll.[105] In fact, Bluebox itself was able to successfully hack to the Barbie App and gain access to the cloud servers. Subsequently, Bluebox suggested that Hello Barbie was vulnerable to a poodle attack,[106] which is "security issue

[101] *Id.*

[102] *Id.*

[103] Samuel Gibbs, *Hackers Can Hijack Wi-Fi Hello Barbie to Spy on Your Children*, GUARDIAN (Nov. 26, 2015 6:16PM), https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children, https://perma.cc/9TNA-QUYE.

[104] *See generally 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, https://perma.cc/5DSA-N75J.

[105] *See id.;* Laura Hautala, *supra* note 11.

[106] Richard Adhikari, *Hello Barbie, Can We Talk About Your Security Issues?*, TECH NEWS WORLD (Dec. 8, 2015 9:27AM), http://www.technewsworld.com/story/82842.html, https://perma.cc/UUC6-9APG.

where a protocol downgrade that allows exploits on an outdated form of encryption."[107] Additionally, Somerset Recon, *explain what Summerset Recon is,* published a two-part "teardown" of Hello Barbie's security systems.[108] The company suggested that the makers of Hello Barbie, Mattel and ToyTalk, failed "to harden their web services."[109] It also suggested that the makers "performed little to no pre-production security analysis and is using their bug bounty program as a low-cost alternative."[110]

3. My Friend Cayla

[24] Genesis Toys and Nuance Communications partnered to create My Friend Cayla an interactive doll. In 2015, Ken Munro hacked the My Friend Cayla doll. He did so to show how vulnerable the doll was despite the Vivid Toy's promises "Cayla is equipped with software to block hundreds of words inappropriate for children."[111] Munro was able to hack

---

[107] Martin Hendrikx, *What is the POODLE Vulnerability and How Can You Protect Yourself?*, HOW-TO GEEK (Oct. 16, 2014), https://www.howtogeek.com/199035/what-is-the-poodle-vulnerability-and-how-can-you-protect-yourself/, https://perma.cc/T2RN-KSJR.

[108] *See Hello Barbie Security: Part 1- Teardown*, *supra* note 104.

[109] Additional vulnerabilities include: "[t]hrough these methods we were able to intercept encrypted communication from the mobile application, trick the mobile application and web application into leaking data, and communicate with ToyTalk servers, masquerading as either Barbie or the mobile application. Minor security weaknesses were found in the device, while larger and more impactful vulnerabilities were found in ToyTalk's web applications and web services. The nastiest vulnerability allows an attacker to enumerate account usernames and brute force their passwords with unlimited retries, without triggering any form of account lockout. There was also a weak password policy in place making this an even more viable attack vector. Additional vulnerabilities include the ToyTalk website issuing password reset requests over HTTP that do not expire, pages vulnerable to Stored Cross-Site Scripting (XSS) and session cookies that did not expire." *Hello Barbie Security: Part 2- Analysis*, SOMERSET RECON J9an. 25, 2016), http://www.somersetrecon.com/blog/2016/1/21/hello-barbie-security-part-2-analysis, https://perma.cc/NJS7-LKM9.

[110] *Id.*

[111] *See* David Moye, *supra* note 14.

Cayla and program the doll to say a number of filthy phrases from Hannibal Lecter and Fifty Shades of Grey containing words (cayla's makers) had deemed inappropriate.[112] In doing so, Munro used a root device to access the doll's Bluetooth system, manipulate the speech database, and make Cayla say the inappropriate phrases.[113] Munro and his research team explained that the hack was so easy because enabling Cayla requires no passcode or pin protection.[114] Shortly after Munro's hack became public, Genesis Toys stated that they had "immediately developed a patch, and upgraded the software,... and we have shipped over 400,000 Cayla's around the globe since its debut last summer, and have not had a single consumer complaint, regarding security issues or problems."[115]

4. CloudPet

[25] Just two months into 2017, the internet connected CloudPets Teddy Bear was hacked. The hackers accessed and held ransom over 2.2 million privately recorded messages between parents and children, emails, and passwords.[116] Over 800,000 people fell victim to this hack.[117] Security researcher Troy Hunt reviewed the Cloud Pet database and found that the company had scant security measures.[118] It did not password protect its

---

[112] *Id.*

[113] Pen Test Partners, *Infosecurity Europe 2015: Cayla Doll Hack Demo*, YOUTUBE (Jun. 18, 2015), https://www.youtube.com/watch?v=XSNOfyqamBo&feature=youtu.be, https://perma.cc/7K3A-M8R8.

[114] *Id.*

[115] *See* David Moye, *supra* note 14.

[116] *See* Rod Chester, *supra* note 15.

[117] *See* Laura Hautala, *supra* note 11.

[118] *See* Troy Hunt, *Data From Connected CloudPets Teddy Bears Leaked and Ransomed, Exposing Kid's Voice Messages*, TROYHUNT.COM (Feb. 28, 2017), https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/, https://perma.cc/SZE5-QSFC.

database, leaving it completely open to hackers.[119] CloudPets has not issued a public response to the hack, nor has it updated its website since 2015.[120] Because the hack occurred recently, there is less information about the hackers and their motives. There is evidence to suggest that this hack was *not* to prove a point, instead it was for ransom.[121]

[26] Before the respective hacks became public, there was little incentive to provide rigorous protection, or to utilize ethical hacking as a preemptive defense mechanism. The attacks brought to light the inadequacies in several of the company's securities systems, which were only addressed after the attacks had occurred. In each case, preemptive measures had not been taken to combat attacks of this nature. It may be too early to tell, but this seems to be a trend: wait for the attacks to occur, and then respond accordingly. Toy manufacturers are not legally held to testing benchmarks or specific security measures for the protection of the digital information gathered by their products.

[27] More specifically, the United States' current privacy and data security laws and correlating regulations provide a patchwork of protection.[122] This patchwork inadequately addresses the need for mandated security testing and benchmarks. For instance, the Children's Online Privacy Protection Act, which focuses on the collect of personal information from a minor under the age of thirteen, requires websites directed at children to provide notice and parental consent obligations.[123] However, the Act fails to assign requirements to toy manufacturers who obviously direct their products towards the same market. The existing laws target specific aspects of data privacy and security procedures, but the implementation of a more holistic legislation has become necessary for

[119] *See id.*

[120] *See id.*

[121] *See* Rod Chester, *supra* note 15.

[122] *See infra* Section III.

[123] *See* Children's Online Privacy Protection Rule, 16 C.F.R. § 312.1 (2017).

smart toys. The next section briefly describes relevant security breach laws and introduces the CPSIA and the toy standards.

III. RELEVANT LAW

[28] The United States takes a very different approach to privacy and data protection when compared to the European Union or Australia. Both the E.U. and Australia utilize an all-encompassing framework[124] to privacy and data protection, however the United States has attempted to extend various laws to cover the holes left by the "patchwork" legislation as it currently stands. The realm of data breaches and cybersecurity attacks in the United States has a rather sparse legal index federally, and seems to be dealt with on a state-by-state basis.[125] A majority of states have implemented post-security breach notification requirements.[126] These requirements vary between states, but all are limited to the period after a customers' proprietary information has been compromised.[127] Additionally, most states do not require a company to report failed attempts to hack their systems.[128] While federal legislation on toy manufacturers remains nonexistent in this context, certain industries like healthcare and securities have specific federal laws regulating the storage

[124] *See* Tom Geller, *In Privacy Law, It's the U.S. vs. the World*, 59 COMM. OF THE ACM, 21, 22 (discussing how U.S. is one of only states to not have one main privacy law, instead the U.S. has several different privacy laws).

[125] *See Security Breach Notification Laws*, NCSL, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx, https://perma.cc/B7MJ-SY7A (last updated Apr. 12, 2017) [hereinafter *Security Breach Notification Laws*].

[126] *See infra* IIIB.

[127] *See id.*

[128] *See* Daniel J. Solove, Article: *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.").

and protections of consumer's personal information.[129] The remainder of this section will discuss laws most relevant to smart toys and data hacks. This section will demonstrate that most privacy laws focus the legal requirements post-data hack rather than implementing specific preventative measures. It should be readily apparent at the end of this section that ensuring customers information is safe, is usually considered to be due diligence of a company.

A. Children's Online Privacy Protection Act ("COPPA")

[29] COPPA is one of two federal laws that regulate and enforce the collection and protection of a minor's personal information. It is also one of the only privacy laws that is preventive, meaning that it deals with the collection of personal information before any type of breach or data hack. All other laws discussed in this Section focus on post-breach or post-data hack measures.

[30] COPPA was passed in Congress to address concerns regarding children's privacy.[130] Prior to COPPA, there were no protections for minors' personal information.[131] The act "prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure

[129] The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Gramm-Leach-Bliley Act, are two examples of federal privacy laws. These federal statutes are very specific and restrict disclosure of protected personal information by imposing security measures. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191 (2017); *see* Gramm-Leach-Bliley Act, Pub.L. 106–102, 113 Stat. 1338 (2017).

[130] *See* David R. Hostetler & Seiko F. Okada, Article: *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, 176 (2013).

[131] *See id.* at 177 ("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.").

of personal information from and about children [under the age of thirteen] on the Internet."[132]

[31] 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.[133] Under COPPA, "operators" are defined 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."[134] These notice and consent requirements must be in place before an entity or individual begins collecting such personal information.[135] Additionally, covered operators and any third parties that collect personal information, must take steps to "protect the confidentiality, security, and integrity of personal information collected from children."[136] It unlikely that such requirements would apply to a toy manufacturer such as Mattel or VTech.

---

[132] Children's Online Privacy Protection Rule, 16 C.F.R. § 312.1 (2017); *see* Daniel Patrick Graham, Article: *Public Interest Regulation in the Digital Age*, 1 COMMLAW CONSPECTUS 97, 124 (2003).

[133] *See* 15 U.S.C. § 6502 (2017); *see* Hostetler & Okada, *supra* note 130, 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." Citations omitted). These 2012 help ensure that companies like ToyTalk are covered.

[134] *See* 15 U.S.C. § 6501(2) (2017).

[135] *Id.*

[136] Children's Online Privacy Protection Act, 16 C.F.R. § 312.8 (2017).

B. Post-Security Breach Notification Laws

[32] On the other end of spectrum, there are post-security breach and data hack laws. Most of these laws are state laws; however, there is one relevant federal law, the Health Information Technology for Economic and Clinical Health Act ("HITECH Act").[137] Because of the rise of Internet, the Internet of Things,[138] and cloud servers,[139] data hacks have become more common. Forty-eight states, "the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information."[140] Notification of breaches must be done in a timely manner according the state law.[141] Interestingly, states provide exemptions in situations where compliance with post-security breach notification is not required.[142]

---

[137] *See, e.g.* CAL. CIV. CODE §§ 1798.29, 1798.82 (2017); *see, e.g.,* VA. CODE ANN. §§ 18.2-186.6, 32.1-127.1:05 (2017); *see infra* note 146.

[138] *See* Jan Henrik Ziegeldorf, Oscar Garcia Morchon & Klaus Wehrle, Privacy in the Internet of Things: Threats and Challenges, Security and Communication Networks 7.12 (2014): 2728-2742 at 1, https://assets.documentcloud.org/documents/2822904/Ziegeldorf-Jan-Henrik-Privacy-in-the-Internet-of.pdf, https://perma.cc/24QY-KMLK.

[139] *See id.* at 4.

[140] *Security Breach Notification Laws*, *supra* note 125 (illustrating that Alabama and South Dakota do not have security breach laws).

[141] Christopher J. Cox & David R. Singh, *Security Breach Notification Las Data Privacy Survey 2014*, WEIL, GOTSHAL & MANGES, LLP, at 5 (2014), http://www.weil.com/~/media/files/pdfs/Weils_Security_Breach_Notification_Laws_Data_Privacy_Survey_2014.pdf, https://perma.cc/L4RN-8J7F [hereinafter *Security Breach Notification Laws Data Privacy Survey 2014*].

[142] "They also provide an exemption from compliance with the statute where a company maintains its own breach notification policy and the policy is consistent with the requirements of the statute." *Security Breach Notification Las Data Privacy Survey 2014, supra* note 141

[33] California was the first state to have a post-security breach notification law and most subsequent states' laws are modeled after it.[143] However, there are variations of definitions and requirements. For example,

> [s]ome states also call for notification of the state attorney general or consumer reporting agencies, depending on the extent of the breach. If a company fails to comply with the breach notification statute, it may be subject to civil penalties enforced by the attorney general; a minority of state statutes also provide for a private cause of action…Some states require consumer notification whenever a breach occurs, while others only require notification if an assessment determines that misuse of the information is likely. Some states permit companies to delay notification pending an investigation to assess the breach and restore the integrity of the data, while others require notification within a certain time period. Even states permitting companies to delay notification for the purposes of investigation have different timing requirements governing when a company must notify consumers after it concludes its investigation. While many states require notice to be provided "without unreasonable delay," other states are much stricter, for example requiring notice to consumers within 45 days of a breach or requiring notification of the appropriate government agency within 10 days. In responding to a data breach situation, special care and expertise are required to analyze and comply with the patchwork of state laws in this area.[144]

[143] M. Scott Koller, Melinda L. McLellan & Jenna N. Felz, *State Law Roundup: Legislatures Across the U.S. Revamp Data Breach Notification Laws*, BAKERHOSTETLER, July 27, 2015, https://www.dataprivacymonitor.com/breach-notification/state-law-roundup-legislatures-across-the-u-s-revamp-data-breach-notification-laws/, https://perma.cc/4UMJ-8JKS; *see Security Breach Notification Laws Data Privacy Survey 2014, supra* note 141.

[144] *Security Breach Notification Laws Data Privacy Survey 2014, supra* note 141, at 5.

[34] As mentioned above, the federal post-security breach and data hack law is HITECH Act. This Act established security breach notification requirements that apply to businesses that handle personal health information and other health information.[145] The HITECH Act applies to all discovered breaches and "include[s] a harm threshold limiting the breach notification requirement to breaches that present a significant risk of harm."[146] Like COPPA, the HITECH Act requires third party service providers to disclose breaches and help provide post-breach services.[147] The HIGHTECH Act and HIPAA,[148] which is not discussed at length in article, may overlap "[t]o the extent a HIPAA covered entity discloses PHI to a cloud provider, it risks exposure to federal data security breach notification requirements under the HITECH Act."[149] While the laws mentioned attempt to canvas the wide realm of post-security breach or data hack reporting requirements for their respective industries, no one privacy law exists that efficiently regulates preventative data hack security measures. Unfortunately, as explained below, the Consumer Product Safety Commission also provides little protection for data security.

C. Consumer Product Safety Improvement Act of 2008

[35] Like COPPA, the Consumer Product Safety Improvement Act of 2008 ("CPSIA") is a preventive law. It requires certain toy manufacturers

[145] Lisa J. Sotto, Bridget C. Treacy & Melinda L. McLellan, *Privacy and Data Security Risks in Cloud Computing*, 15 ELECTR. COMMERCE & L. REP. 186, 186 (2010), https://www.hunton.com/files/Publication/4845e31f-63d8-4f9a-9a36-a074e4170225/Presentation/PublicationAttachment/6f52b2fd-2973-48cc-9f23-c941f1e19358/Privacy-Data_Security_Risks_in_Cloud_Computing_2.10.pdf, https://perma.cc/3Q7H-7278.

[146] *Id.; see also* THE HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT, Pub. L. 111-5, 123 Stat. 258-263 (2017).

[147] *See* THE HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT, Pub. L. 111-5, 123 Stat. 258-263 §13407 (2017).

[148] HIPAA restricts service providers in the health insurance field from disclosing customer's personal information to an unreliable third party. Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191 (2017).

[149] Lisa J. Sotto, Bridget C. Treacy & Melinda L. McLellan, *supra* note 145.

to meet toy safety standards before releasing it to consumers. CPSIA was passed by Congress in 2008, in response to massive Chinese product recalls.[150] The Act aimed to protect American consumers from defective products made abroad.[151] The Consumer Product Safety Commission, an independent government agency, ("CPSC") was derived from the Consumer Product Safety Act,[152] a previous act created to "protect the public from unreasonable risks of injury or death from thousands of types of consumer products under the agency's jurisdiction."[153] The CPSIA applies to children's products designed for children 12 years old and younger.[154] It imposes substantive requirements such as:

- Lead content in accessible components (100 ppm);
- Lead in paint and surface coatings (90 ppm);
- Phthalates (0.1% per banned phthalate) – Toys and Child Care Articles (Sleeping & Feeding) Only; and
- Toy Safety Standard (ASTM F963).[155]

[36] Key process requirements for children's products primarily intended for children 12 years old and younger:

- Third party testing by CPSC-accepted labs

[150] *See* Eileen Flaherty, *Comment: Safety First: The Consumer Product Safety Improvement Act of 2008*, 21 LOY. CONSUMER L. REV. 372, 372–73 (2009).

[151] *See id.*

[152] *See id.* ("Congress created the CPSC in 1972 under the Consumer Product Safety Act."); *see* Consumer Product Safety Act, 15 U.S.C., §§ 2051−2089 (2017).

[153] Eileen Flaherty, *supra* note 153, at 390 ("The Consumer Product Safety Act grants the CPSC the power to set mandatory product safety standards, ban dangerous products from the marketplace, order product recalls, and levy fines against violators. Despite the CPSC's enforcement powers, in 2007 it was understaffed, underfunded, and charged with regulating an ever-increasing number of imported goods.").

[154] *See* TOY SAFETY UPDATE DRAFT, U.S. CONSUMER PRODUCT SAFETY COMMISSION, at 1, (Apr. 2017), https://www.toyassociation.org/App_Themes/tia/pdfs/safety/ChinaSafetySeminar12/cohen-en.ppt, https://perma.cc/QTT4-QUYA.

[155] *Id.* at 2.

- Conformity certificates issued by importers & manufacturers (Children's Product Certificate)
- Tracking labels
- New safety rules for durable infant products:
- Cribs; infant walkers; bath seats; toddler beds; play yards; bed rails; additional items every six months
- Product registration cards[156]

[37] The CPSIA also "requires manufacturers of non-children's products to issue a General Certificate of Conformity ("GCC")."[157]

[38] Since 2009, the CPSIA has required all toys manufactured in the United States of America to comply with the toy safety standard and requirements of Toy Safety ASTM (explain abbreviation and quote it) F963.[158] The ASTM creates and updates its toy safety standards through a committee on consumer products. The committee "is comprised of a dedicated group representing industry, government, consumers, academia, and other interested parties."[159] The standard, F963: "includes requirements and test[ing] methods to prevent potential injuries such as choking, sharp edges, toxins, pinching, and other potential hazards."[160] Further, the standard was revised in 2016 to add and revise existing standards. F963-16 also adds:

- new labeling requirements for toys that have certain small coin/button batteries,
- temperature and current-limiting requirements for lithium-ion batteries, and

[156] *Id.*

[157] *Id.*

[158] ASTM INT'L QUICK FACTS, ASTM INT'L, https://www.astm.org/toys.html, https://perma.cc/B95J-8ZVD (last visited Apr. 16, 2017).

[159] *Id.*

[160] *Id.*

- new requirements for materials and toys that could expand if accidentally swallowed.[161]

[39] Other revisions include:

- new soaking and compression tests for magnets
- new requirements and clarifications related to microbiological safety;
- clarifications to heavy elements requirements for toy substrate materials
- revised requirements for toys involving projectiles; and,
- clarification of requirements and supplemental guidance for impact hazards.[162]

IV. HOW TO INCENTIVIZE ADDITIONAL SECURITY TESTING

[40] The previous section demonstrates that the current patchwork of privacy and post-security breach notification laws do not sufficiently incentivize toy manufacturers to increase safety measures. In fact, the negative publicity and correlating sales declines from a data hack seems to be the only incentive for companies to increase data safety measures, and exclusively in a reactive fashion. This section proposes an amendment to the ASTM-963-11, which is a substantive requirement of CPSIA, to require smart toy manufacturers to conduct additional safety testing via ethical hacking, to help increase safety and reduce vulnerabilities. While many people consider CPSIA's function to be protect consumers against imported toys, the Act could inadvertently serve as the best vehicle to regulate the security for smart toys such as Hello Barbie and My Friend Cayla.

[41] This article does not propose mandated hacking as an amendment to COPPA. This is because COPPA focuses more on parental notice and consent requirements than preventative measures for hacks and data breached. It does require an operator to have reasonable protections in place but to add the provisions of mandated ethical hacking would

[161] *Id.*

[162] *Id.*

overwhelm the heart of the statute. The CPSIA and ASTM-963-11 is a better location for the proposed language below because it focuses on toy safety. Even though it has to do with physical safety and toxic materials, this extension to smart toys follows a natural progression of toy safety.

A. Proposal

[41] More specifically, that the Toy Safety Standard ASTM F963-11 be amended to include a smart toy testing requirement. The proposed language should be inserted following Section 4.5 "Sound Producing Toys." This new section, titled Smart Toys, should include the following language and subparts: definitions, scope, labeling, manufacturing requirements, and testing requirements.

Section 4.6 Smart Toys

ii. Definitions

1. **Bluetooth:** means a wireless technology standard that is used to exchange data over short distance (less than 30 feet), usually between personal mobile devices.[163]
2. **Children:** means a minor under that is younger than of thirteen years of age.
3. **Comparable Skills:** means an individual who has similar or same qualifications of a certified ethical hacker[164]
4. **Connected to Technology:** means any toy, game, virtual learning product, or article that utilizes the internet via Wi-Fi or Bluetooth, or other technologies.[165]

[163] *See* Tara Struyk, *What is the Difference Between Bluetooth and Wi-Fi?*, TECHOPEDIA, (Apr. 28, 2016), https://www.techopedia.com/2/27881/networks/wireless/what-is-the-difference-between-bluetooth-and-wi-fi, https://perma.cc/T5UA-4KDF.

[164] *See Process Eligibility*, EC-Counsel, https://cert.eccouncil.org/application-process-eligibility.html, https://perma.cc/9YGK-BKKF (last visited Apr. 18, 2017).

[165] Other technologies can include "breath to bytes."

5. **Ethical Hacking:** means testing conducted by a specialist in the field of information technology and must be versed in the following: "footprinting and reconnaissance, scanning networks, enumeration, system hacking, Trojans, worms and viruses, sniffers, denial-of-service attacks, social engineering, session hijacking, hacking web servers, wireless networks and web applications, SQL injection, cryptography, penetration testing, evading IDS, firewalls, and honeypots."[166]
6. **Smart Toys:** means any toy, game, virtual learning product, or other article designed, labeled, advertised, or otherwise intended for use by children which is intended to be Connected to Technology.[167]
7. **Smart Toys Manufacturer:** entity or individual that is in the business of manufacturing toys that are connected to the internet and utilize other technologies. This entity or individual need not specialize in only Smart Toys, it only has to produce a single smart toy and intend to release it to the market.
8. **Wi-Fi:** means high-speed access to the Internet.[168]

iii. Scope

1. This section sets forth the requirements for smart toys intend for the use by children as defined above.[169]

iv. Testing Requirements

[166] *See* Ed Tittel, *Best Information Security Certifications For 2017*, TOM'S IT PRO (Dec. 13, 2016 5:28AM), http://www.tomsitpro.com/articles/information-security-certifications,2-205-3.html, https://perma.cc/GQ9B-LMRE.

[167] 16 C.F.R. § 1505.1 (2017).

[168] *See* Tara Struyk, *supra* note 163.

[169] 16 C.F.R. § 1505.2 (2017).

1. **General**
    a. Smart toys shall be produced in accordance with detailed material specifications, production specifications, and quality assurance programs. Quality assurance programs shall be established and maintained by each manufacturer to assure compliance with all requirements of this part.
        i. Quality assurance programs will maintain and execute the ethical hacking testing requirements as discussed in Section (2)(a).

    b. The manufacturer or importer shall keep and maintain for 3 years after production or importation of each lot of toys (i) the material and production specifications and the description of the quality assurance program required by paragraph (1)(a) of this section, (ii) the results of all inspections and tests conducted, and (iii) records of sale and distribution. These records shall be made available upon request at reasonable times to any officer or employee of the Consumer Product Safety Commission. The manufacturer or importer shall permit such officer or employee to inspect and copy such records, to make such inventories of stock as he deems necessary, and to otherwise verify the accuracy of such records.

2. **Ethical Hacking**
    a. A smart toy shall be tested, prior to market release, to identify system vulnerabilities, to access points for penetration, and to prevent unwanted access to network and

information systems.[170] After such issues are determined by the hacking, a report of vulnerabilities and weaknesses must be prepared and kept on file for the amount specified in Section (1)(b).

b. Ethical hacking must be conducted in accordance with current industry standards. Suggested forms of testing are web application and network penetration testing, website security assessments, wireless network audits, web application testing, secure code reviews, intelligence audits, and social engineering.[171]
c. Companies may utilize a non-certified hacking professional but must utilized an individual or team of individuals with comparable skills.

[42] This amendment to the ASTM-963-11 does not address the labeling and manufacturing requirements of smart toys. Specifically, this proposal lays out the preventative testing requirements for smart toys. The labeling and manufacturing requirements of electrical toys,[172] can be adopted and revised to fit smart toys rather easily; however, this is beyond the scope of this article. Additionally, this proposal does not require a specific timeline for testing nor does it require a third-party service to conduct the testing. It is highly encouraged for companies to use a third party if it does not have the proper resources. However, if a company has proper resources it may do so internally.

[170] *See* Ed Tittel, *supra* note 166.

[171] *See Penetration Testing*, PEN TEST PARTNERS, https://www.pentestpartners.com/penetration-testing-services/penetration-testing/, https://perma.cc/8Y9L-3LJD (last visited Apr. 10, 2017); *see Pentration Testing & Ethical Hacking Services*, WIZLYNX GROUP, https://www.wizlynxgroup.com/us/about.html, https://perma.cc/5PC7-R32K (last visited Apr. 10, 2017).

[172] *See* 16 C.F.R. § 1505.4 (2017).

B. Compliance with New Testing Requirements

[43] Smart toy manufacturers, like the ones discussed in this article, can comply with this new testing requirement rather easily. Because many of these companies are either working with a qualified information technology ("IT") company or have their own skilled IT department, an existing employee or contractor may be able to conduct this ethical hacking. Unlike other types of toy safety testing standards, this proposal does not require the use of a third-party.[173] Thus, companies such as VTech could hire a cyber-security specialist that is certified in hacking.[174] This particular employee could conduct and develop a report to help eliminate any vulnerabilities before the product is released to the market. Similarly, these companies can hire one of the many hacking companies that do this on a regular basis. Such hacks cost anywhere from $4,000 to $20,000.[175] While the cost may seem exorbitant, the correlating cost of a reported data breach after a company fails to preventively hack will be incalculably more significant.

C. Advantages and Disadvantages of Proposal

[44] This section addresses the potential benefits and challenges to this proposal. Some may argue that the time and costs of implementing such a testing requirement will be too high, and that those costs will negatively impact sales. As previously discussed above, the costs of implementing these testing requirements will be fairly low, especially when compared to

[173] Small objects, toys that contain plastic film and cords, toys that contain flammability components require third party testing. *See* ASTM F 963-11 REQUIREMENTS, CONSUMER PRODUCT SAFETY COMMISSION, https://www.cpsc.gov/Business--Manufacturing/Business-Education/Toy-Safety/ASTM-F-963-11-Chart/, https://perma.cc/JK4T-LX9S (last visited Apr. 20, 2017).

[174] *See Certified Ethical Hacking Certification*, EC-COUNCIL, https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/, https://perma.cc/T49S-3SU6 (last visited Apr. 19, 2017); *see also* Ed Tittel, *supra* note 166.

[175] *See* Gary Glover, *How Much Does a Pentest Cost?*, SECURITY METRICS BLOG, http://blog.securitymetrics.com/2015/04/penetration-test-cost.html, https://perma.cc/3H9V-UZBS (last visited Apr. 10, 2017).

the plausible costs associated with a data hack. Many of the companies that manufacture smart toys are already skilled in technology and data privacy, so they could likely conduct the testing internally. Those who do not have a skilled individual can hire a certified hacker or contract services with an ethical hacking company. Others may argue that the government has no place setting safety standards because of the big brother argument as well as their lack of technological knowledge. Further, these companies have already faced harsh criticizes for their toys. These smart toys already face lower sales because of their negative public image.

[45] Additionally, critics may argue that the testing requirements will only encourage hackers to be more creative. Once the hackers figure out what the companies are testing for, they will mutate and find newer ways to target the toys. However, this is not necessarily the case. The testing requirements do not require *specific* name tests.[176] It suggests various tests but will require these companies to follow industry standard. This is to ensure the testing keeps with the pace of technological advancements. Critics could also suggest that the customer has assumed the risk of data hacks when purchasing the doll. However, in this case the freedom of contract argument is flawed because a child is not competent under law to enter into a contract. Under the proposed amendments to ASTM-963-11 the child is directly protected from the data breaches. The contract is likely between the parent/guardian and company and the parent's information is not being stolen, this proposed legislation would extend protection beyond the consumer, to the user, a minor. A final potential concern would be what remedies should be made available to consumers or users if the ethical hacking fails? In determining those remedies it would have to be determined what specific standards are required to hold the manufacturing company, or the individual hacker assigned with the preventative hack, to be held liable. This is a particularly valid concern because the Computer Fraud and Abuse Act does not provide legal protections for ethical hackers.

[46] The proposed amendment has many positive implications. The most simplistic and important effect is that the amendment could potentially prevent a hacker from stealing personal information about an

[176] See *supra, Sec*tion IVA.

innocent child using a smart toy. As internet technologies continue to advance an incredible rate, increasing numbers of smart toys will be released into the market. This preventive and cost-effective amendment to prevent data hacks is an efficient solution to combat the inevitable increase in data hack attempts. Regardless of legislative implementation, companies that voluntarily implement a preventative ethical hacking defense system will inevitably receive a boost in the public perception of their product. If these companies show that they have complied with the national toy standard, they will seem more secure and reputable generally. It should be noted that Congress has initiated the recognition of the problem of data hacking in smart toys. In December 2016, the Committee on Commerce, Science, and Transportation released a report titled "Children's Connected Toys: Data Security and Privacy Concerns."[177] This report called attention to the vulnerabilities of these toys and recommended that "toymakers should build in effective security from a [c]onnected [t]oy's inception."[178] The report does not provide specific instructions or guidance on what effective security would be but the proposed amendments herein would provide the "effective security" the report recommended. Effective security can be established and maintained through mandated ethical hacking under CPSIA.

V. CONCLUSION

[47] Mandated ethical hacking is a potential way to enforce stringent security protections on smart toy manufacturers in a clear, efficient manner. This proposal will benefit both the toy manufacturer as well as the general public by protecting company public image and protecting minors' personal information. This ethical hacking requirement will even benefit companies like ToyTalk and VTech who have been the subject of data hacks and the correlating negative public image in the past. This article and proposal aims to incite thought and action to prevent and lower the number of data hacks of children's personal information.

[177] BILL NELSON, CHILDREN'S CONNECTED TOYS: DATA SECURITY AND PRIVACY CONCERNS, STAFF OF OFFICE OF OVERSIGHT AND INVESTIGATIONS MINORITY 1 (2016) https://www.billnelson.senate.gov/sites/default/files/12.14.16_Ranking_Member_Nelson_Report_on_Connected_Toys.pdf, https://perma.cc/V25H-ZEAS.

[178] *Id.* at 9.