Washington Journal of Law, Technology & Arts

Volume 14 | Issue 2 Article 2

4-1-2019

Animal Healthcare Robots: The Case for Privacy Regulation

Sulaf Al-Saif

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 14, ISSUE 2 SPRING 2019

ANIMAL HEALTHCARE ROBOTS: THE CASE FOR PRIVACY REGULATION*

*Sulaf Al-Saif***

CITE AS: 14 WASH. J.L. TECH. & ARTS 77 (2019)

http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/1876/14WJLTA077.pdf

ABSTRACT

Animal healthcare robots are a form of healthcare or wellness devices that possess the appearance of animals or pets and that collect data on the user. The appearance, use, and nature of data collected by these robots illustrate two types of devices for which privacy regulation falls short: Internet of Things ("IoT") devices and healthcare devices. This paper surveys the animal healthcare robots currently in the market, details the special privacy concerns associated with such robots, examines the current state of potentially relevant privacy laws, and makes recommendations for privacy regulation in the future.

TABLE OF CONTENTS

** Sulaf Al-Saif, University of Washington School of Law, Class of 2020. Thank you to Professors Ryan Calo, William Covington, and Cindy Jacobs for the guidance, and to Jacob Magit, Casey Yamasaki, and Sydney Finlay for the advice and support.

INTRODUCTION

Healthcare robots are increasingly prolific, and increasingly "social." Today, the trending iteration of such "social" healthcare robots is interactive animal robots. Animal healthcare robots, because of their approachable, cute appearance, and their low-maintenance nature (as opposed to a real pet), are touted as a replacement for animal-assisted therapy and indeed, research shows the efficacy of such robots.[1] Animal healthcare robots are currently being used to assist senior citizens with dementia and children with a range of diseases like diabetes, autism, and cancer.[2] For the purposes of this paper, anthropomorphic or zoomorphic robots (e.g. those with eyes and limbs) are included under the umbrella of animal healthcare robots because they exhibit similar physical characteristics, at least as they relate to privacy.

There have been calls for more privacy regulation of medical

[1] Moyle et al., *Effect of an Interactive Therapeutic Robotic Animal on Engagement, Mood States, Agitation and Psychotropic Drug use in People with Dementia: a Cluster-Randomised Controlled Trial Protocol*, BMJ Open (Aug. 12, 2015) https://bmjopen.bmj.com/content/5/8/e009097.

[2] Rudie Obias, *10 Therapy Robots Designed to Help Humans*, Mental Floss (Dec. 30, 2015) http://mentalfloss.com/article/71987/10-therapy-robots-designed-help-humans.

devices[3] and Internet of Things ("IoT") devices.[4] Animal healthcare robots fall within both of these categories. Due to their characteristics, use, and prevalence, these robots present unique privacy concerns that have gone largely unaddressed by regulators. These concerns are not alleviated by the current state of privacy regulation. This paper surveys the range of animal healthcare robots and their uses, the privacy concerns associated with these robots, and potentially applicable privacy laws, and argues for the need for regulation to address these concerns.

I. SURVEY OF ANIMAL HEALTHCARE ROBOTS AND THEIR USES

For the purposes of this paper, "animal healthcare robots" are robots that possess the characteristics of an animal (whether realistic or not), and that are used for therapeutic purposes through social human-robot interaction. There are two broad types of animal healthcare robots that this paper will focus on: (1) those targeting the elderly (particularly those with dementia), and (2) those targeting children with conditions such as autism, diabetes, or cancer.

A. Robots targeting the elderly

Of the robots targeting the elderly (and of healthcare animal robots generally), Paro the Seal has gained some notoriety due to being featured in the TV shows *The Simpsons* and *Master of None*.[5] Paro is a fluffy seal robot the size of a human baby which contains

[3] Christopher Frenz, *Healthcare privacy plans need to account for medical device security*, IAPP (Apr. 14, 2017) https://iapp.org/news/a/healthcare-privacy-plans-need-to-account-for-medical-device-security/.

[4] IEEE, *Should the Government Regulate IoT Devices?,* IEEE Innovation, https://innovationatwork.ieee.org/should-government-regulate-iot/ (last accessed June 1, 2019).

[5] Sheree Joseph, *Yes, PARO the Baby Seal Robot from Master of None,* Daily Life (Jan. 14, 2016) http://www.dailylife.com.au/dl-people/dl-entertainment/yes-paro-the-baby-seal-robot-from-master-of-none-is-real-20160114-gm5l2a.html; Anna Silman, *The Scoop on PARO, the Breakout Seal From 'Master of None',* Thrillist (Nov. 23, 2015) https://www.thrillist.com/entertainment/nation/paro-the-seal-creator-interview-master-of-none.

five sensors for "tactile, light, audition, temperature, and posture."[6] It can recognize being stroked or held, the direction and tone of voice, whether its environment is light or dark, and imitates the sound of a baby harp seal.[7] More importantly, Paro can recognize its name, greetings, and praise, and learns the preferred behavior of the user and if hit after a certain action, it will refrain from that behavior in the future.[8] It is utilized primarily for patients with dementia, and has been shown to positively affect their behavioral and psychological symptoms.[9] As of March of 2019, Paro's manual indicates that it has no internet or Bluetooth connectivity features.[10]

Another notable set of devices, Joy for All Companion Pets, was developed by Hasbro to provide companionship to the elderly and is designed to look, act, and feel like a real pet.[11] Joy for All Pets come in two categories: a robot cat and a robot dog.[12] Similarly to Paro, the Joy for All Companion Pets have no connectivity features, as indicated by the manual.[13]

In contrast, Care-o-bot 3 is a robot manufactured by Fraunhofer, a German research organization, and is designed to help seniors live independently.[14] Care-o-bot 3 is programmed to know where items are in a user's home, and through a phone app or using the robot's

---

[6] PARO, *PARO Therapeutic* Robot, http://www.parorobots.com/.

[7] *Id.*

[8] *Id.*

[9] Carolyn Crist, *Families of Dementia Patients See Positive Effect of Social Robot Seal*, Reuters (Dec. 14, 2017) https://www.reuters.com/article/us-health-dementia-paro-robot/families-of-dementia-patients-see-positive-effect-of-social-robot-seal-idUSKBN1E837G.

[10] *PARO Manual* (Sep. 2015) http://www.parorobots.com/pdf/PARO%20Manual-2015-09.pdf.

[11] Joy for All, *Our Story*, https://joyforall.com/pages/our-story (last accessed June 1, 2019).

[12] *Id.*

[13] *Joy for All Companion Pets Care Guide*, https://joyforall.zendesk.com/hc/en-us/articles/360004213453-Joy-for-All-Companion-Pet-Pup-Care-Guide (last accessed June 1, 2019).

[14] Jenny McGrath, *This Polite, Drink Fetching Robot may one day be a Grandparent's Best Friend*, Digital Trends (Feb. 6, 2015) https://www.digitaltrends.com/home/the-care-o-bot-3-robot-helps-seniors-live-independently/.

touchscreen, the user can order the robot to fetch an item.[15] It is also used for communication and entertainment purposes; the user can make video calls through the robot's screen, and the robot can play music or remind the user of appointments through its speakers.[16] Finally, the robot can provide emergency assistance by navigating towards a fallen user and enabling video or audio calls to emergency services.[17] Care-o-bot 3 has an amorphous, rectangular shape, with two arms, one for manipulation (e.g. grabbing items) and another for interaction (a touchscreen allowing both input and output).[18] Care-o-bot 3 is equipped with a 3D sensor allowing it to detect visual and audio signals from its surroundings,[19] as well as Wi-Fi connectivity.[20] In response to users' weariness of interacting with the robot, Fraunhofer created Care-o-bot 4, a much "cuter" and aesthetically pleasing iteration of Care-o-bot 3 that is equipped with internet connectivity and the ability for use as a general home assistant.[21]

---

[15] Fraunhofer, *Care-o-bot 3: Application*, Fraunhofer, https://www.care-o-bot.de/en/care-o-bot-3/application.html.

[16] *Id.*

[17] *Id.*

[18] Kwc, *Robots Using ROS: Care-O-bot* 3, ROS (March 10, 2010) http://www.ros.org/news/2010/03/robots-using-ros-care-o-bot-3-fraunhofer-ipa.html.

[19] Fraunhofer, *Care-o-bot 3: Product Vision of a Robotic Home Assistant*, https://www.care-o-bot.de/content/dam/careobot/en/documents/productsheets/Product%20Sheet_Care-O-bot%203.pdf.

[20] Fraunhofer, *Care-o-bot 3: Hardware: Technical* Data, https://www.care-o-bot.de/en/care-o-bot-3/hardware/technical-data.html.

[21] Jenny McGrath, *This Polite, Drink Fetching Robot may one day be a Grandparent's Best Friend*, Digital Trends (Feb. 6, 2015) https://www.digitaltrends.com/home/the-care-o-bot-3-robot-helps-seniors-live-independently/; Fraunhofer, *Care-o-bot 3: Hardware: Technical Data*, https://www.care-o-bot.de/content/dam/careobot/en/documents/technicaldata/Care-O-bot%204_Technical_Data.pdf; Evan Ackerman, *Care-o-bot 4 Is the Robot Servant We All want but Probably Can't Afford* (Jan. 29, 2015) https://spectrum.ieee.org/automaton/robotics/home-robots/care-o-bot-4-mobile-manipulator.

B. Robots targeting children

Utilizing a typically friendly appearance and similarity to both pets and stuffed animals, animal healthcare robots are often targeted towards children. Sproutel, a healthcare research and development company, developed two robots: My Special Aflac Duck and Jerry the Bear, aiming to give children undergoing treatment for cancer and type 1 diabetes a calming and educational companion.[22]

My Special Aflac Duck is a duck robot designed to provide companionship and entertainment to children undergoing cancer treatment.[23] Children can engage in medical play, mirroring the treatments they are undergoing (IV fluids, drawing blood, and chemotherapy) by administering them to the robot.[24] In addition, the child can engage in nurturing play by feeding and bathing the duck.[25] For both the medical and nurture play, the duck comes equipped with a mixed-reality app for a more immersive experience.[26] Further, the Aflac duck can express emotions like sadness and happiness when tapped with an attached "emoji card," can emit music and calming noises when prompted by the app, and can respond to touch and sound stimuli which prompt it to breathe, nuzzle, and sing.[27] Finally, it can sense when other Aflac ducks are within a five-foot radius of and react with a "brief quacking conversation."[28] My Special Aflac Duck is distributed to children in hospitals free of charge.[29]

---

[22] Stephanie Baum, *In Collaboration with Aflac, Sproutel Develops Companion Robot Duck to Help Kids with Cancer*, MedCity News (May 10, 2018) https://medcitynews.com/2018/05/companion-robot-for-kids-with-cancer/.

[23] Aflac Childhood Cancer Campaign, *My Special Aflac Duck: Learn More*, https://aflacchildhoodcancer.org/learn.cfm.

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] GMA Team, *Meet My Special Aflac Duck who Brings Smiles to the Faces of Kids Fighting Cancer*, ABC News (Sep. 17, 2018) https://abcnews.go.com/GMA/Wellness/meet-special-aflac-duck-brings-smiles-faces-kids/story?id=57624406.

Similarly, Jerry the Bear is a robot with the appearance of a teddy bear designed as a companion for children with type 1 diabetes.[30] It helps educate children about the importance of healthy behavior like proper nutrition through its accompanying app, and allows the child to simulate medical play by drawing Jerry's blood, measuring his blood sugar levels, and giving him insulin injections.[31] Jerry the Bear is equipped with Wi-Fi connectivity and multiple interactive storylines, allowing children to guide him through daily routines.[32]

BUDDY the emotional robot was developed by Blue Frog Robotics, and is described by its creators as a "real Swiss Army knife" capable of a broad range of uses in the home, such as controlling security and smart home devices; providing multimedia entertainment like music, video, and photography through its camera; personal assistive capabilities like appointment reminders; elder care through monitoring and video call capabilities; social interaction through "mobile telepresence" and the ability to post to social media; and the ability for customization by the installation of compatible apps and accessories.[33] Blue Frog Robotics collaborated with Auticiel, a French educational software development company, to create an app integrated into BUDDY that allows children with autism to learn social cues through interactive gameplay.[34]

---

[30] Jerry the Bear, *Jerry the Bear: A Comforting Companion for Children With Type 1 Diabetes*, https://www.jerrythebear.com/.

[31] Ginger Vieira, *"Jerry the Bear" for Kids with Type 1 Diabetes: New & Improved!,* Diabetes Daily (March 29, 2017) https://www.diabetesdaily.com/jerry-the-bear-stuffed-toy-kids-with-type-1-diabetes.

[32] Healthline Editorial Team, *Meet Jerry the Bear*, Healthline (Nov. 24, 2015) https://www.healthline.com/health/type-1-diabetes/jerry-the-bear#1.

[33] Buddy The Emotional Robot, *Buddy the First Emotional Companion Robot*, https://buddytherobot.com/en/buddy-the-emotional-robot/.

[34] Steve Crowe, *How Buddy is Helping Autistic Children*, Robotics Business Review (Dec. 1, 2015) https://www.roboticsbusinessreview.com/rbr/how_buddy_is_helping_autistic_children/.

II. SPECIAL PRIVACY CONCERNS WITH ANIMAL HEALTHCARE ROBOTS

A. Targeting of vulnerable populations

Animal healthcare robots are mainly targeted towards the elderly (and particularly those with diseases like dementia), and children (and particularly those with conditions like autism), two populations with potentially compromised physical, mental, or emotional states. Research indicates that humans suffering from loneliness, such as patients with dementia, are more likely to anthropomorphize (or attribute human characteristics or behavior to) robots.[35] Research has also shown that children ascribe feelings like happiness or sadness to their toys that possess lifelike features.[36] Children are also much more likely than adults to be persuaded by robots.[37] Although children with autism struggle to connect with human stimuli, they exhibit a more positive and trustful reaction towards robots with pet-like or cartoon-like features.[38]

Therefore, it is especially concerning that the users targeted by animal healthcare robots are those who are more likely to ascribe a degree of personhood to them, and less likely to perceive them as machines capable of collecting, storing, and transmitting granular data.

---

[35] Meera Lee Sethi, *Human Beings have a Deep-Seated Tendency to Humanize Everything Around Them. Is it Delusion – or a Natural and Healthy Response to Loneliness?*, Greater Good Magazine (June 1, 2008) https://greatergood.berkeley.edu/article/item/seeing_human.

[36] Naveed Saleh, *Which Toys Do Children Anthropomorphize?,* Psychology Today (Dec. 22, 2015) https://www.psychologytoday.com/us/blog/the-red-light-district/201512/which-toys-do-children-anthropomorphize.

[37] University of Plymouth, *Robots Have Power to Significantly Influence Children's Opinions*, Science Daily (Aug. 15, 2018) https://www.sciencedaily.com/releases/2018/08/180815154454.htm.

[38] Cbibihan et al., *Why Robots? A Survey on the Roles and Benefits of Social Robots in the Therapy of Children with Autism*, International Journal of Social Robotics (2013), https://arxiv.org/pdf/1311.0352.pdf.

B. Lifelike appearance of robots builds a sense of trust and intimacy

In general, when humans interact with a robot with "likeable" and lifelike features, they tend to trust the robot when interacting with it.[39] A study on human interactions with anthropomorphic autonomous vehicles shows that humans in an anthropomorphic vehicle reported trusting the vehicle, being more relaxed in the event of an accident, and being less likely to blame the vehicle for any incidents.[40] Another study has shown that owners of the Roomba, an autonomous robotic vacuum (with no lifelike features except for the ability to move autonomously and sense obstacles), have developed an emotional attachment to it, name their robots, and even pre-clean for them.[41] The more lifelike a robot is, the more likely humans are to self-promote in its presence (e.g., giving more to charity in the presence of a lifelike robot).[42] This has the potential of harming one of the central tenets of privacy: safeguarding people's ability to be themselves in times and places of solitude.[43]

Animal healthcare robots are intentionally designed to encourage familiarity, engagement, and socialization with the robots. Japanese roboticist Masahiro Mori's "uncanny valley" theory is that robots that look and behave almost like humans, but not quite, can cause revulsion and uneasiness.[44] This is why robot

---

[39] Ghazali et al., *Effects of Robot Facial Characteristics and Gender in Persuasive Human-Robot Interaction,* Frontiers in Robots and AI (June 21, 2018) https://www.frontiersin.org/articles/10.3389/frobt.2018.00073/full.

[40] Epley et al., *The Mind in the Machine: Anthropomorphism Increases Trust in an Autonomous Vehicles*, Journal of Experimental Social Psychology (May 2014) https://www.researchgate.net/publication/260007895_The_Mind_in_the_Machine_Anthropomorphism_Increases_Trust_in_an_Autonomous_Vehicle.

[41] Charlie White, *Roomba Driving Owners Crazy with Anthropomorphic Robot Love*, Gizmodo (Oct. 2, 2007) https://gizmodo.com/roomba-driving-owners-crazy-with-anthropomorphic-robot-306248.

[42] Ryan Calo, *Robot Ethics: The Ethical and Social Implications of Robots,* Robots and Privacy (Apr. 2, 2010) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1599189.

[43] *Id.*

[44] Yisela Alvarez Trentini, *The Uncanny Valley in Game Design*, Medium

design follows the principle that a robot with human features is likely to be perceived as endearing as long as it doesn't have too many human characteristics.[45]

For instance, the creator of Paro designed it as a baby harp seal because although it's soft and appealing, it's not a familiar pet (like a dog) which would increase the likelihood of people with cognitive disorders having preconceived notions about it, making them more likely to believe it's a true animal.[46] In addition, BUDDY the robot was designed with "cuteness" as the end goal to increase users' desire to interact with and take care of it: it is designed to have the physical characteristics of a human baby, such as a small size, large eyes, a disproportionately large head, a rounded body, and short limbs.[47] Hence, animal healthcare robots are designed with the end goal of familiarity, trust, and engagement in mind by appearing un-machine-like, which could potentially reduce user awareness of device functions like data collection.

C. Potential collection of health information

The importance of privacy in healthcare spaces has been emphasized from ancient times to the present, as evinced, for example, by the Hippocratic oath that physicians must take to protect patients' healthcare information.[48] The concept of privacy in an individual's health information is borne in part out of respect to the patient's vulnerability and dignity in such a setting, and a desire

(Mar. 8, 2019) https://towardsdatascience.com/the-uncanny-valley-in-game-design-6a6c38a36486.

[45] *Id.*

[46] Lee Williamson, *How a Cute Robot Seal Called Paro is Bringing Cheer to Dementia Patients,* Alpine HC Group (Jun. 1, 2017) https://alpinehc.co.uk/blog/cute-robot-seal-paro-bringing-cheer-dementia-patients/.

[47] Blue Frog Robots, *Why Robots Need to Be Cute?*, http://www.bluefrogrobotics.com/en/why-robots-needs-to-be-cute/.

[48] Majmuder and Guerrini, *Fedeal Privacy Protections: Ethical Foundations, Sources of Confusion in Clinical Medicine, and Controversies in Biomedical Research*, AMA Journal of Ethics (Mar. 2016) https://journalofethics.ama-assn.org/article/federal-privacy-protections-ethical-foundations-sources-confusion-clinical-medicine-and/2016-03.

to protect patients from exploitation.[49]

Hospitals, and by extension, health care facilities like nursing homes, are public places where "very private things happen."[50] The respect given to privacy in these facilities is shown by the fact that, for example, patients and their loved ones can request private rooms for consultations or conversations with healthcare staff in most facilities.[51] The use of IoT medical devices to assist and monitor homebound or institutionalized individuals with disabilities requires the generation of massive amounts of health data to be gathered and analyzed, creating a heightened risk of the exposure or unauthorized access to such data.[52]

There are special considerations when dealing with medical or healthcare IoT devices, particularly because they collect data in real time. For instance, one researcher hypothesized that although a consumer may use a fitness tracker solely for wellness-related purposes, the data could be used to make inferences about the user's health, life span, and therefore suitability for credit or employment.[53] The FTC has noted that healthcare IoT devices are increasingly equipped with third party applications capable of collecting and transmitting sensitive information about bodies, habits, and behaviors without the user's knowledge.[54] Moreover, such sensor data is particularly hard to fully anonymize because

---

[49] *Id.*

[50] Erinn Connor, *6 Things You Need to Know About Patient Privacy Rights*, Everyday Health, https://www.everydayhealth.com/news/6-things-you-need-know-about-patient-privacy-rights/.

[51] *Id.*

[52] Wassnaa AL-mawee, *Privacy and Security Issues in IoT Healthcare Applications for the Disabled Users a Survey,* Master's Theses (2012) https://scholarworks.wmich.edu/cgi/viewcontent.cgi?article=1661&context=masters_theses.

[53] FTC Staff Report, *Internet of Things: Privacy & Security in a Connected World,* FTC (Jan., 2015) https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[54] *FTC Warns of Security and Privacy Risks in IoT Devices,* Pindrop Blog, https://www.pindrop.com/blog/ftc-warns-of-security-and-privacy-risks-in-iot-devices/.

each dataset created about the individual is inherently unique, meaning efforts to protect privacy through anonymity are largely futile.[55]

Animal healthcare robots are equipped with a wide range of sensors, and can detect a wide range of data such as light, touch, and sound. Even if direct health information, like disease or genetic information, is not being directly collected, it is possible to make inferences about personal life expectancy and real-time health status from simple information like body temperature, breathing, pulse, and blood pressure.[56] The advent of artificial intelligence means such inferences are getting increasingly smarter, faster, and more accurate.[57]

For example, Paro's sensing of light can be used to make inferences about sleep patterns, and the usage of My Special Aflac Duck's "emoji card" can create inferences by tracking the child's mood over time. Thus, even sensing of data that appears unrelated to health can be used to make increasingly more accurate inferences about a person's health, and that merits reasonable privacy protections even of such basic data collected by animal healthcare robots.

D. Increase in market for connected animal healthcare robots

The rise in the use of IoT devices in healthcare, and specifically for elder care, indicates an increased likelihood that more—if not all—animal healthcare robots will be equipped with connectivity functions in the future. The healthcare IoT market is growing rapidly; one estimate forecasts a compound annual growth rate of

---

[55] Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 Tex. L. Rev. 85, 130 (2014).

[56] Kang and Larkin, *Inference of Personal Sensors in Internet of Things,* International Journal of Information, Communication Technology and Applications (Jan., 2016) http://dro.deakin.edu.au/view/DU:30080976.

[57] Michael Copeland, *What's the Difference Between Deep Learning Training and Inference?*, Nvidia (Aug. 22, 2016) https://blogs.nvidia.com/blog/2016/08/22/difference-deep-learning-training-inference-ai/.

31.1% by 2024,[58] and McKinsey forecasts spending on medical IoT software applications to reach $1 trillion by 2025.[59] In addition, because of increased life expectancy, the elder care market in 2018 was estimated to be worth a staggering $863 billion and growing,[60] and the use of IoT for elder care is forecasted to increase in the coming years.[61] As such, market trends point towards increased use of connected IoT technology in healthcare, and specifically in the elder care market.

Although the user manuals for Paro and the Joy for All Companion Robot indicate that they do not possess connectivity features, as opposed to the other robots surveyed in this paper, their success is indicative of increasing acceptance and proliferation of animal healthcare robots. Paro has gained international success and attention, and was even puzzlingly dubbed the "world's most therapeutic robot" by the Guinness Book of Records in 2002.[62]

Although animal healthcare robots appear to occupy a smaller, niche portion of the medical IoT sector, advancements and growth in the sector, as well as the demonstrated global success of robots like Paro, indicate that this type of robot will be increasingly commonplace, although this area remains almost wholly unregulated.

E. Use in homes, hospitals, and nursing homes

---

[58] Chris Nerney, *Market for Healthcare IoT to See Strong Growth, report predicts,* Connected Care Watch (Sep. 26, 2018) http://www.connectedcarewatch.com/news/market-healthcare-iot-see-strong-growth-report-predicts.

[59] Ezgi Tasdemir, *IoT Revolution in Healthcare*, Medium (Mar. 11, 2018) https://medium.com/@ezgitasdemir/iot-revolution-in-health-care-901fec5459cf.

[60] Anna Codrea-Rado, *How Smart Home Technology is Empowering Seniors and Combating Social Isolation*, Dell Techologies (Jan. 16, 2018) https://www.delltechnologies.com/en-us/perspectives/how-smart-home-technology-is-empowering-seniors-and-combating-social-isolation/.

[61] Philip Regenie, *IoT, the Smart Home, and Elderly Care,* Medium (May 1, 2017) https://medium.zanthion.com/iot-the-smart-home-and-elderly-care-34b296d8ddb1.

[62] *Cuddly Robot Comforts the Elderly*, Trends in Japan, https://web-japan.org/trends/09_sci-tech/sci090917.html.

In discussions of privacy around the globe, there is consistent emphasis on one's right to privacy in his or her own home.[63] The U.S. Supreme Court held that people have a reasonable expectation of privacy, free from government intrusion, in their own homes.[64] This concept is recognized internationally: for example, the United Nations Universal Declaration of Human Rights states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence."[65] Thus, the technological intrusion on privacy in the home is of special concern, because such an intrusion of "machines that our brains understand as people into historically private spaces may reduce already dwindling opportunities for solitude."[66]

Even small devices in the home can generate a vast amount of data. One manufacturer indicated that the 10,000 households using its in-home IoT product can generate 150 million discrete data points a day, which translates into approximately one data point every six seconds for each household.[67] Such granular data collection over time can generate inferences about things like sensitive behavior patterns, sleep patterns, levels of exercise, progression of Parkinson's disease, mood, and even gender.[68]

Thus, the entry of animal healthcare robots into residences, nursing homes, and hospitals merits special concern about the data generated through daily activity that is surreptitiously being collected by these robots.

---

[63] Daniel J. Solove, *Understanding Privacy*, GWU Law School Public Law Research Paper No. 420 at 4 (May, 2008), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888.

[64] *Id.* at 2.

[65] *Id.* at 3-4.

[66] Ryan Calo, *Robot Ethics: The Ethical and Social Implications of Robots*, Robots and Privacy (Apr. 2, 2010) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1599189.

[67] FTC Staff Report, *Internet of Things: Privacy & Security in a Connected World,* FTC at 13 (Jan., 2015) https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[68] *Id.* at 14.

III. SURVEY OF POTENTIALLY APPLICABLE PRIVACY LAWS

The United States does not have a single national data protection law; instead, privacy is protected via common law and state laws, as well as industry-specific federal laws and regulations.[69] In a landmark decision, the Supreme Court held in 1965 that the right to privacy can be derived by implication from the "penumbra" of the Constitution.[70] Several states like California, Washington, and Florida have added a right to privacy to their constitutions.[71]

A. HIPAA "Privacy Rule"

The Privacy Rule of the Health Insurance Portability and Accountability Act ("HIPAA") was published in 2002 by the Department of Health and Human Services ("HHS"), and was promulgated in part due to rising concern about the increased use of computers and automated systems for healthcare records, as well as the increased number of parties involved in healthcare treatment, payment, and oversight.[72]

There are three types of entities covered by HIPAA. First, health care providers, who are paid to provide health care. This includes doctors, hospitals, and nursing homes; but the entities are covered only if they transmit healthcare information electronically in connection with covered transactions.[73] Second, health plans, which

---

[69] ICLG, *Data Protection 2018 | USA*, International Comparative Legal Guides (Dec. 6, 2018) https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.

[70] Griswold v. Connecticut, 381 U.S. 479, 485-86 (1965).

[71] NCSL, *Privacy Protections in State Constitutions*, National Conference of State Legislature (Nov. 7, 2018) http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.

[72] *A Brief Summary of the HIPAA Medical Privacy Rule*, Every CRS Report (April 10, 2002 – April 30, 2003) https://www.everycrsreport.com/reports/RS20934.html.

[73] Privacy Rights Clearinghouse, *Health Privacy: HIPAA Basics* (March 12, 2019) https://www.privacyrights.org/consumer-guides/health-privacy-hipaa-basics#covered%20entities.

pay the cost of healthcare. This includes health insurance companies, employer-sponsored group health plans, and government-sponsored health insurance like Medicaid.[74] Finally, health clearinghouses, who process information for transmission in a standard format between covered entities, and act as a go-between for health plans and health providers and rarely interact with patients.[75]

In addition to these covered entities, business associates of a covered entity may be covered by HIPAA.[76] Business associates are organizations that have access to health information in order to provide a service or function on behalf of a covered entity.[77] There is a wide range of services that business associates provide, such as legal, actuarial, data aggregation and analysis, and certain patient safety activities.[78]

Device manufacturers can potentially be covered by HIPAA, but only if they interact with a covered entity or a business associate in some way, such as when the device sends personal health data to the healthcare provider.[79] However, if the manufacturer of the medical device or application interacts directly with the user, HIPAA protections would not apply.[80]

In the case of animal healthcare robots, they are, for the most part, purchased directly from the manufacturer or distributer to the user. Nothing in the manuals for animal healthcare robots indicates that the data collected by them is sent to nor viewed by healthcare providers or other covered entities, nor used in the course of formal

---

[74] *Id.*

[75] *Id.*

[76] *Id.*

[77] Elizabeth Snell, *How Do HIPAA Regulations Apply to Wearable Devices*, Health IT Security (March 23, 2017) https://healthitsecurity.com/news/how-do-hipaa-regulations-apply-to-wearable-devices.

[78] Privacy Rights Clearinghouse, *Health Privacy: HIPAA Basics* (March 12, 2019) https://www.privacyrights.org/consumer-guides/health-privacy-hipaa-basics#covered%20entities.

[79] Elizabeth Snell, *How Do HIPAA Regulations Apply to Wearable Devices*, Health IT Security (March 23, 2017) https://healthitsecurity.com/news/how-do-hipaa-regulations-apply-to-wearable-devices.

[80] *Id.*

healthcare or treatment.

The exception to this is My Special Aflac Duck, which is distributed free of charge directly to pediatric cancer wards in hospitals.[81] Therefore, it could potentially fall under the ambit of manufacturers that interact with HIPAA covered entities, and thus need to be HIPAA-compliant themselves. Nothing on My Special Aflac Duck's website indicates that it strives to meet requirements for HIPAA compliance.[82] Although Aflac itself is an insurance company that is HIPAA-compliant, nothing indicates that data collected by its robot follows the same safeguards.[83]

Therefore, it appears that since the majority of animal healthcare robots are merely consumer products with minimal interactions from any covered entity, HIPAA does not provide the requisite privacy protections for the robots.

B. FDA Regulation

The Food and Drug Administration ("FDA") is a federal agency responsible for promoting health through, *inter alia*, the pre-market approval of medical devices.[84] The term "device" is defined by the Federal Food Drug & Cosmetic ("FD&C") Act as:

> "[A]n instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is . . . intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals . . ."[85]

---

[81] Cision, TIME Magazine Honors Innovative My Special Aflac Duck, PR Newswire (Nov. 19, 2018) https://www.prnewswire.com/news-releases/time-magazine-honors-innovative-my-special-aflac-duck-300752625.html.

[82] Aflac Childhood Cancer Campaign, *My Special Aflac Duck: Learn More*, https://aflacchildhoodcancer.org/learn.cfm.

[83] Aflac, *Privacy Policy*, https://www.aflac.com/about-aflac/privacy-policy.aspx.

[84] U.S. Food & Drug Administration, *What We Do* (March 28, 2018) https://www.fda.gov/AboutFDA/WhatWeDo/default.htm.

[85] 21 U.S.C. § 321(h)(2).

The FDA does not have any privacy or cybersecurity requirements for manufacturers of medical devices, but does issue cybersecurity guidelines for the industry.[86]

Only Paro is advertised as an FDA-approved medical device.[87] The rest of the animal healthcare robots are not FDA-approved, and even if they were, the FDA does not offer the stringent privacy protections required to mitigate the concerns associated with these robots.

C. California's IoT Law and CCPA

Although not federal, California's IoT law is the most relevant in the context of animal healthcare robots. The law was passed in September of 2018 and comes into effect in January of 2020.[88] The bill requires any company that manufactures, or contracts to manufacture "connected devices" that are sold or offered for sale in California to equip the devices with "reasonable security features."[89] At a minimum, the security features must be compatible with the nature and function of the device, appropriate to the type of data being collected, and designed to protect the information on the device from "unauthorized access, destruction, use, modification, or disclosure."[90]

Although the bill was criticized for being too vague, making it hard for manufacturers to comply, it's still seen as a step in the right

---

[86] U.S. Food & Drug Administration, *Medical Devices: Cybersecurity* (March 1, 2019) https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm.

[87] *Paro Robots positions stuffed animal as therapeutic device,* Medtech Insight (Nov. 30, 2009) https://medtech.pharmaintelligence.informa.com/MT028223/Paro-Robots-positions-stuffed-animal-as-therapeutic-device.

[88] Taylor P. Widawski, *California Passes Internet of Things Law,* Cyber Law Monitor, https://www.lexology.com/library/detail.aspx?g=f60d8841-6c15-4c92-8c00-157916d2e916.

[89] *Id.*

[90] *Id.*

direction.[91] The bill contains cybersecurity requirements, but does not contain provisions pertaining to privacy.[92] In addition, California's IoT law may have an effect on the national IoT regulation efforts due to a phenomenon called the "California effect."[93] Due to economic integration, there is a tendency to ratchet regulatory standards upward to comply with the most stringent jurisdiction's law.[94] This means states could follow suit by creating or increasing standards similar to those in California.

Another potentially applicable law is the California Consumer Privacy Act ("CCPA") of 2018, which similarly comes into effect in January of 2020.[95] The Act requires companies that collect personal information and that are either over a certain revenue threshold, collect personal information from 25,000 California households or more, or derive fifty percent or more of its revenues from sale of personal information to provide consumers with particular rights.[96] These rights include disclosure to the consumer of the personal information collected, giving the consumer the right to access and delete personal data (with exceptions), and requires businesses to create a privacy policy.[97]

Although CCPA may apply to manufacturers of animal healthcare robots, and may induce other jurisdictions to follow suit through the California effect, the market for animal healthcare robots appears to be small enough to evade the CCPA.

Therefore, although California's IoT and CCPA laws are a step in the right direction, they are not comprehensive enough, are

---

[91] *Id.*

92 . Cal. Civ. Code § 1798.91.04 (effective Jan, 1, 2020).

[93] Perkins and Neumayer, *Does the 'California Effect' Operate Across Borders? Trading- and Investing-up in Automobile Emissions Standards*, 19 Journal of European Public Policy 2 (Sep. 1, 2011) https://www.tandfonline.com/doi/full/10.1080/13501763.2011.609725?scroll=top&needAccess=true.

[94] *Id.*

[95] Melissa J. Krasnow, *A Summary of the California Consumer Privacy Act of 2018,* IRMI (Sep., 2018) https://www.irmi.com/articles/expert-commentary/a-summary-of-ccpa-of-2018.

[96] *Id.*

[97] *Id.*

limited to one jurisdiction, and it is unclear what compliance would look like because they have yet to come into effect.

D. FTC's Section 5 Bar on Unfair and Deceptive Practices

The Federal Trade Commission ("FTC") uses Section 5 of the FTC Act to prohibit "unfair or deceptive acts or practices in or affecting commerce."[98] When companies violate consumer privacy rights, or fail to provide adequate cybersecurity measures, the FTC uses its Section 5 power to bring legal action against these companies and to enforce consumer rights.[99]

Although Section 5 is a powerful tool to enforce consumer privacy rights, it only applies prospectively and requires a showing of injury.[100] This means that it does not require manufacturers to equip their devices with any privacy safeguards, but allows legal action against them if failure to provide such safeguards results in injury to the consumer.

An example of the FTC's *ex post facto* privacy enforcement is *In re Vizio, Inc., Consumer Privacy Litigation*, a federal class action lawsuit brought against a manufacturer of smart TVs equipped with software that clandestinely collected content viewing histories and sold the data to advertisers.[101] Among the data collected and sold were consumer IP address, zip code, region, and language settings.[102] The plaintiffs alleged that the totality of information Vizio collected could link each individual with an accurate history of their content viewing behavior, that the data collection feature was automatically enabled in the device, and that Vizio's data collection and dissemination practices were not disclosed in

---

[98] 15 U.S.C. § 45(a)(1).

[99] Federal Trade Commission, *Privacy and Security Enforcement*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

[100] Federal Trade Commission, *How Does the FTC Protect Consumer Privacy and Ensure Data Security?* (Jan., 2017) https://www.ftc.gov/reports/privacy-data-security-update-2016#how.

[101] *In re* Consumer Privacy Litigation of *Vizio, Inc.,* 238 F.Supp.3d 1204 (2017).

[102] *Id.* at 1212.

marketing or privacy policies.[103] A California district court ruled that the plaintiffs' invasion of privacy and intrusion upon seclusion tort claims under the California Constitution and the Massachusetts Privacy Act survived the defendants' motion to dismiss.[104] Eventually, Vizio settled with the plaintiffs for $17 million.[105] It also entered a consent decree with the FTC which required Vizio to disclose and obtain affirmative consent for its data collection and dissemination practices, refrain from misrepresenting the privacy and security of the consumer information collected, and to delete data collected in violation of privacy law.[106]

Apart from litigation, the FTC issues staff reports and industry guidelines to help manufacturers avoid violating consumer privacy, but they are only recommendations and do not have binding effect.[107] Therefore, the FTC does not sufficiently mitigate the privacy concerns associated with animal healthcare robots by requiring manufacturers to ensure certain safeguards are in place prior to sale and distribution.

Although Section 5 enforces privacy breaches between the device owners and the manufacturers, it falls short in protecting third-parties' data collected by the devices, such as guests in the home.[108] This makes it ill-suited to protect from privacy issues arising from the "Internet of Other People's Things."[109] Therefore, the data collected on, for example, the family, guests, or nursing home or hospital staff that surround the owner of an animal

---

[103] *Id.* at 1212-13.

[104] *Id.* at 1232-33.

[105] Dorothy Atkins, *Vizio Cuts $17M Deal To End Smart-TV Spring MDL*, Law 360 (Oct. 4, 2018) https://www.law360.com/articles/1089511.

[106] FTC, *Vizio to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent*, FTC (Feb. 6, 2017) https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.

[107] FTC Staff Report, *Internet of Things: Privacy & Security in a Connected World*, FTC (Jan., 2015) https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[108] Margot E. Kaminski, Matthew Rueben, William D. Smart & Cindy M. Grimm, *Averting Robot Eyes*, 76 MD. L. REV. 983, 1000 (2017).

[109] *Id.*

healthcare robot would not be covered by FTC's Section 5 powers.

IV. RECOMMENDATIONS FOR A REGULATORY SCHEME

Animal healthcare robots are an illustration of the shortcomings of federal privacy regulation, as they encompass the concerns associated with the growing IoT device market as well as the connected healthcare device market. This paper does not call for a regulation of these devices themselves, but rather a technologically neutral regulation. Technology neutrality is a principle that applies to regulation in the internet, telecoms, and data protection areas, and has three meanings: (1) technical standards designed to limit negative externalities like safety should describe the result to be achieved, and leave companies free on how to achieve that result; (2) some regulatory principles should apply regardless of the type of technology used; or (3) regulators should not use regulation to push the market towards a structure they find optimal (i.e., they should not pick "technological winners").[110]

The optimal regulatory scheme that addresses the privacy concerns of animal healthcare robots would apply results-oriented privacy requirements to the broader IoT and healthcare device industries. A suitable framework informing such a regulation should be in line with the Fair Information Practice Principles ("FIPPs"), which is an internationally recognized set of principles and guidelines that inform regulation for data protection and privacy.[111] The four most pertinent FIPPs in IoT and connected device privacy regulation are: (1) purpose specification, (2) use limitation, (3) notice and transparency, and (4) data minimization and security.[112]

---

[110] Bourreau and Maxwell, *Technology Neutrality in Internet, Telecoms and Data Protection Regulation*, Computer and Telecommunications L. Rev. (Nov. 24, 2014) http://dx.doi.org/10.2139/ssrn.2529680.

[111] Pam Dixon, *A Brief Introduction to Fair Information Practices,* World Privacy Forum (Jun. 5, 2006) https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/.

[112] Center for Democracy and Technology, *Comments after November 2013 Workshop on the "Internet of Things"*, at 5-6 (Jan. 10, 2014) https://cdt.org/files/pdfs/iot-comments-cdt-2014.pdf.

IoT and connected device manufacturers should have an affirmative obligation to clearly and conspicuously disclose to the consumers the types and amounts of data being collected, as well as the transfer, purpose, and use of such data.[113] This notice and transparency requirement allows consumers, regulators, and advocates to learn more about manufacturers' privacy practices and to hold the companies responsible in the case of non-compliance, whether by market forces, private causes of action, or legislation.[114] Furthermore, manufacturers should be obligated to use the collected data solely for the use and purpose specified or a future use that falls within the context of the device's purpose.[115] This means manufacturers are prohibited, without the consumer's informed consent, from transferring or selling the data to third parties or utilizing it for a purpose other than the one disclosed to the consumer.[116] In addition, manufacturers should not collect nor retain more data than is necessary for the purpose of the device, and should not be able to make broad and vague statements about those purposes like "product improvement" or "research" to skirt the use limitation requirement.[117] Finally, the manufacturer should equip the device with reasonable security features, such as limited data retention and routine deletion, provision of security updates, de-identification (ensuring collected data cannot be traced back to a specific user), and user control.[118]

Another overarching principle that should be followed in regulating devices like animal healthcare robots is a requirement of "privacy by design." The concept was developed by Dr. Ann Cavoukian, a former Canadian Information and Privacy Commissioner, and is based on the view that privacy cannot be assured by compliance with regulatory frameworks alone, but should be companies' default mode of operation.[119] Privacy by

---

[113] *Id.*
[114] *Id.*
[115] *Id.*
[116] *Id.*
[117] *Id.* at 7.
[118] *Id.* at 8-10.
[119] Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles* (Jan.

design means privacy should be integral to organizational priorities, design processes and planning operations.[120] The 7 principles of privacy by design are: (1) proactive not reactive, meaning data breaches should be anticipated and prevented before they occur; (2) privacy by default, meaning the manufacturer is responsible for ensuring personal data is protected; (3) privacy being embedded into the product design in a "creative and holistic" manner; (4) full functionality by accommodating user-friendliness as well as privacy and security interests; (5) end-to-end security, meaning data is protected from the moment it enters the system, is retained, and subsequently destroyed; (6) visibility and transparency by allowing the user access to how the information moves through the system; and (7) respect for user privacy by making user privacy the number one concern.[121]

The body best equipped to regulate machines like animal healthcare robots is the FTC. This is because Congress empowered the FTC with a broad, vaguely-defined, and flexible mandate to address consumer protection, particularly in the sphere of privacy.[122] The breadth of Section 5 would allow it to react to challenges created by new technologies, and to provide a safety net for privacy concerns falling outside of existing laws.[123] Further, the FTC is equipped with a well-developed body of jurisprudence and expertise related to privacy and robotics, including mandated disclosures, design-based solutions, and organizational procedures and data protection.[124] The FTC's established body of law built up over more than a century and its accommodation of new technologies with a light regulatory touch and deference to industry expertise means it's

---

2011) https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

[120] Search Encrypt, *7 Principles of Privacy by Design,* Medium (Nov. 20, 2017) https://medium.com/searchencrypt/7-principles-of-privacy-by-design-8a0f16d1f9ce.

[121] *Id.*

[122] Woodrow Harzog, *Unfair and Deceptive Robots*, 74 Maryland L. Rev. 785, 812 (May 5, 2015) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2602452.

[123] *Id.* at 813-14.

[124] *Id.* at 815-16.

particularly well-situated to regulate consumer privacy for devices like animal healthcare robots.[125]

In addition to the FTC's broad regulation of privacy for IoT devices, the FDA should provide supplementary regulation in the sphere of privacy and cybersecurity for connected medical devices. The FTC has a long history of cooperating with agencies like the FDA in matters like certain advertisements for food and drugs.[126] While the FDA has authority to enforce (and has long enforced) non-deceptive advertising for drugs, it has not issued guidance on medical device promotion.[127] In addition, the FDA exempts devices it categorizes as low-risk, "general wellness products" from regulation.[128] However, due to the aforementioned concerns, the FDA should require manufacturers of connected healthcare robots that wish to advertise their products as FDA-approved medical devices (like Paro does) to comply with privacy and security requirements similar to those of the FTC. These requirements should be imposed in the pre-market approval ("PMA") stage, and the FDA should review the product's privacy and cybersecurity protections as a part of its PMA review.[129]

V. CONCLUSION

Animal healthcare robots are a welcome innovation that could provide accessible companionship, education, and general wellness to a class of people that are unable, by virtue of their age and condition, to receive the full benefits of human- or pet-assisted therapy, or who wish to supplement it. However, they reveal major shortcomings in federal privacy regulation of two rapidly growing

---

[125] *Id.* at 824-828.

[126] *Id.* at 830.

[127] Thomas Sullivan, *FDA: The Differences with Pharmaceutical and Device Promotion Standards,* Policy & Medicine (May 6, 2018) https://www.policymed.com/2013/11/fda-the-differences-with-pharmaceutical-and-device-promotion-standards.html.

[128] *FDA Creates Unregulated Device Category for General Wellness Products*, FDANews (Feb. 20, 2015) https://www.fdanews.com/articles/170055-fda-creates-unregulated-device-category-for-general-wellness-products.

[129] U.S. Food & Drug Administration, *Premarket Approval (PMA*) (last updated Feb. 21, 2019) https://www.fda.gov/MedicalDevices/ucm2007514.htm .

markets: IoT devices and connected healthcare devices. The nascent dangers on consumer privacy created by these devices create a need and an opportunity for federal agencies, by virtue of their history, flexibility, and expertise, to enact broad privacy regulation. The FTC and the FDA should collaborate to create a technology-neutral consumer privacy regulation that bridges the gap left unaddressed by existing federal privacy laws. Although it's difficult to assess the privacy risks associated with animal healthcare robots and similar machines, it's better to anticipate and prevent potential harm and to provide a safety net for consumers in an increasingly connected and rapidly evolving world.