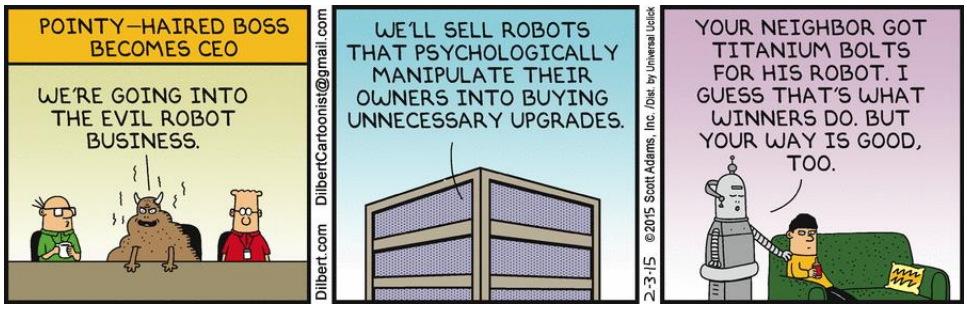
UNFAIR AND DECEPTIVE ROBOTS

Woodrow Hartzog[*]



Robots like household helpers, personal digital assistants, automated cars, and personal drones are or will soon be available to consumers. These robots raise common consumer protection issues, such as fraud, privacy, data security, and risks to health, physical safety and finances. Robots also raise new consumer protection issues, or at least call into question how existing consumer protection regimes might be applied to such emerging technologies. Yet it is unclear which legal regimes should govern these robots and what consumer protection rules for robots should look like.

The thesis of the article is that the FTC's grant of authority and existing jurisprudence make it the preferable regulatory agency for protecting consumers who buy and interact with robots. The FTC has proven to be a capable regulator of communications, organizational procedures, and design, which are the three crucial concepts for safe consumer robots. Additionally, the structure and history of the FTC shows that the agency is capable of fostering new technologies as it did with the Internet. The agency defers to industry standards, avoids dramatic regulatory lurches, and cooperates with other agencies. Consumer robotics is an expansive field with great potential. A light but steady response by the FTC will allow the consumer robotics industry to thrive while preserving consumer trust and keeping consumers safe from harm.

---

[*]Associate Professor, Samford University's Cumberland School of Law; Affiliate Scholar, Center for Internet and Society at Stanford Law School.

CONTENTS

INTRODUCTION

It turns out it is tough to spot your own vulnerabilities. This year a South Korean woman was sleeping on the floor when her robot vacuum ate her hair, forcing her to call for emergency help.[1] The mobile dating app Tinder has been infiltrated by bots posing as real people that attempt to socially manipulate users into downloading other apps, disclose credit card information, and use webcams.[2] When remotely controlled anthropomorphic robots, which appear to be acting autonomously, are introduced to children, young ones become attached to the robot and will disclose secrets to the robot that they would not tell their parents or teachers.[3] Should companies be required to tell people how vulnerable they are? Should companies be required to design safer robots? Thus far, there is no consensus regarding the regulatory response to consumer robotics. If this uncertainty is not already a problem, it soon will be.

Robots are now in the hands of consumers. Household helpers, personal digital assistants, automated cars, personal drones, and countless other robots are or will soon be available to consumers for a reasonable price. Yet it remains unclear exactly how vulnerable consumers are to these robots. It is also unclear which legal regimes should govern these robots and what consumer protection rules for robots should look like.

---

[1] See Matthew Humphries, *Fire department called after robot vacuum 'attacks' sleeping owner*, GEEK (Feb. 6, 2015, 10:28), http://www.geek.com/news/fire-department-called-after-robot-vacuum-attacks-sleeping-owner-1615192/; *see also*, Brian Ashcraft, *Robot Vacuum Attempts to Chew Owner's Head Off*, KOTAKU (Feb. 6, 2015, 7:00 AM), http://kotaku.com/robot-vacuum-attempts-to-chew-owners-head-off-1684171465.

[2] *See* Leo Kelion, *Tinder accounts spammed by bots masquerading as singles*, BBC (Apr. 2, 2014, 7:59 ET), http://www.bbc.com/news/26850761; *see also*, Satnam Narang, *Tinder: Spammers Flirt with Popular Mobile Dating App.*, SYMANTEC (Jul. 1, 2013).

[3] *See e.g.*, Jacqueline Kory Westlund & Cynthia Breazeal, *Deception, Secrets, Children, and Robots: What's Acceptable?*, The Emerging Policy and Ethics of Human Robot Interaction. In Proceedings of the 10th ACM/IEEE Conference on Human-Robot Interaction (HRI), 2015, http://www.openroboethics.org/hri15/wp-content/uploads/2015/02/Mf-Westlund.pdf; C.L. Bethel ET AL., *Secret-Sharing: Interactions between a Child, Robot, and Adult*. Proceedings of the 2011 IEEE International Conference on Systems, Man, and Cybernetics, 2489–2494, http://www.cindybethel.com/publications/IEEESMC2011-BethelCL.pdf; Breazeal, C.L., DESIGNING SOCIABLE ROBOTS (2004); M. Fior ET AL., *Children's Relationships with robots: Robot is child's new friend*, 4 JOURNAL OF PHYSICAL AGENTS 9 (2010).

Robots for consumers present two kinds of challenges. First, many of these robots raise common consumer protection issues, such as fraud, privacy, data security, failure to exercise reasonable care and the exploitation of the vulnerable. Like computers, robots are capable of collecting, using, and disclosing information in harmful ways. Robots can also be hacked. Second, the coming wave of robotics also raises new consumer protection issues, or at least calls into question how existing consumer protection regimes might be applied to such foreign technologies.

The Federal Trade Commission (FTC) is responsible for protecting consumers through its authority under Section 5 of the FTC Act to police unfair and deceptive trade practices. The FTC's recent expansion into the "Internet of Things" and the mass adoption of robots by consumers are about to meet head-on. But is the FTC the best agency to protect consumers who purchase and use robots? What should the FTC's consumer robotics jurisprudence look like?

The goal of this paper is to explore the proper role of the FTC regarding consumer robotics. This paper will identify the consumer vulnerabilities created by robots and analyze existing FTC jurisprudence to determine what standards, if any, can guide the design and use of robots that are capable of being used to physically, emotionally, and financially harm consumers.

I argue that that the FTC's grant of authority and existing jurisprudence make it the preferable regulatory agency for protecting consumers who buy and interact with robots. The FTC has proven to be a capable regulator of communications, organizational procedures, and design, which are the three crucial concepts for safe consumer robots. The FTC's existing framework for protecting consumers from fraud, data breaches, privacy harms, and exploitation is robust enough to adequately protect consumers and clear enough to notify commercial entities of their obligations when designing, selling, and using robots that interact with consumers.

Additionally, the structure and history of the FTC shows that the agency is capable of fostering new technologies as it did with the Internet. The agency consistently defers to industry standards, avoids dramatic regulatory lurches, and shares authority with other agencies. Consumer

robotics is an expansive field with great potential. A light but steady regulatory approach by the FTC will allow the consumer robotics industry to thrive while preserving consumer trust and keeping consumers safe from harm.

This article proceeds in three parts. Part I surveys the potential vulnerabilities created by consumer robotics. This part explores different kinds of problematic consumer robots such as spybots, nudgebots, scambots, automated algorithms, and cyborgs. It maps concerns about data security, exploitation, privacy, and deception onto the existing FTC Section 5 jurisprudence, which prohibits unfair and deceptive trade practices.

Part II will explore the FTC's background and jurisdiction. While the FTC is limited to regulating robots in commerce, it has great discretion over who and what to regulate. Robot designers, merchants, and organizations using robots as part of a service must refrain from unfair and deceptive trade practices. The FTC has also developed a "means and instrumentalities" theory of secondary liability to reach entities that facilitate consumer deception or harm.

Part III addresses the question of agency choice. Is the FTC the best agency to regulate consumer robotics? Should it be the only regulator of consumer robotics? I conclude that the FTC should take the lead on consumer robotics issues because the agency has an established body of law to draw from, it can accommodate nascent technologies, it gives deference to industry standards, it is capable of responding to technological change quickly but with stability, and that it can use Section 5 as a safety net for issues not specifically addressed elsewhere. I also conclude that the FTC should try to regulate consumer robotics in isolation. The agency should work with other federal and state agencies and possibly even new agencies like a proposed Federal Robotics Commission to ensure that consumers are protected from unfair and deceptive robots.

I. CONSUMER ROBOTS RAISE EXISTING AND NEW CONSUMER PROTECTION ISSUES

What is a robot anyway? It is difficult to say. There is no settled definition for the term "robot," particularly in law and policy circles.[4] Do robots have to be embodied, or can software "bots" be counted as a robot? Do robots have to be automated, or can telepresence machines that are remotely operated be counted as a robot?

Neil Richards and William Smart have noted "In most [common examples of robots], the robots can move about their world and affect it, often by manipulating objects. They behave intelligently when interacting with the world. They are also constructed by humans. These traits are, to us, the hallmarks of a robot."[5] Richards and Smart propose the following working definition: "A robot is a constructed system that displays both physical and mental agency, but is not alive in the biological sense."[6]

This definition is a good place to start. However, for purposes of discussing consumer protection policy, it can be too narrow. Often non-embodied and non-autonomous technologies will present similar or related consumer protection issues to those contemplated by Richards and Smart's definition. The functional difference between robot and automated technology can sometimes be hard to articulate. Thus, for the purposes of this article, I will also include certain automated software and non-automated technologies.

In many ways, robots are not exceptional regarding consumer protection issues. Robots can be used to lie, scam, pressure, and manipulate consumers in ways that are analogous to existing fraudulent practices. Ian Kerr presciently warned in 2004, "Like Hollywood's finest directors, who are able to steer their audiences' attention away from the false assumptions that they have so skillfully engendered, some software programmers are applying principles of cognitive science to develop electronic entities that garner consumer trust. Unfortunately, some e-

---

[4] Neil M. Richards & William D. Smart, How Should the Law Think About Robots?, In Proceedings at We Robot 2012, University of Miami, http://robots.law.miami.edu/wp-content/uploads/2012/03/RichardsSmart_HowShouldTheLawThink.pdf.
[5] *Id.* at 5.
[6] *Id.*

businesses are exploiting these applications to garner trust where no such trust is warranted."[7] Kerr called this the *Californication of commerce*, and his concern about consumer vulnerability to autonomous agents which leverage cognitive science for manipulative purposes is squarely a consumer protection issue.[8]

However, in many ways, robots are exceptional with respect to consumer protection. In a series of articles, Ryan Calo has described how robots will challenge, among other regulatory schemes, existing consumer protection regimes such as privacy and notice because they are capable of physical harm, have emergent properties, and feel to humans like social actors.[9]

Should robots designed with personalities and human or animal-like faces be subject to different rules than simple boxes with wheels? At what degree of automation should designers no longer be liable for the decisions made by their autonomous agents? For example, should the designer of a software bot whose function is to make random online purchases be liable for when the bot buys drugs on the black market?[10] Should software terms of use be subjected to more scrutiny when they govern mechanical body parts like implanted hearing aids and electronic

---

[7] Ian Kerr, Bots, Babes, and the Californication of Commerce, 1 U. OTTAWA L. & TECH. J. 285 (2004).

[8] *Id.*

[9] Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. (forthcoming 2015); *see also*, Ryan Calo, *People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship*, 114 PENN. ST. L. REV. 809 (2010); Ryan Calo, *Open Robotics*, 70 MD. L. REV. 571 (2011); Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027 (2012); M. Ryan Calo, *Robots and Privacy, in* ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS 187, 194 (Patrick Lin, Keith Abney & George A. Bekey ed. 2012).

[10] *See* Ryan Calo, *A Robot Really Committed a Crime. Now What?*, FORBES (Dec. 23, 2014, 6:04 PM), http://www.forbes.com/sites/ryancalo/2014/12/23/a-robot-really-committed-a-crime-now-what/; Daniel Rivero, *Robots are Starting to Break the Law and No One Knows What to do About It*, FUSION (Dec. 29, 2014), http://fusion.net/story/35883/robots-are-starting-to-break-the-law-and-nobody-knows-what-to-do-about-it/.

body parts?[11] Should robot salespeople be subject to different rules than their human counterparts?[12]

This part will explore the different consumer protection issues presented by robotics. Where appropriate it will also describe potentially relevant prior FTC jurisprudence and established concepts. It will also highlight areas of uncertainty and where more law, policy, and theory is needed. Some of these robots are not designed to harm consumers, they are just used that way. For others, consumer harm and deception is the reason for the robot's existence. While some robots may be an immediate threat to consumers, others merely serve as proofs-of-concept or harbingers for future problems.

1. *Scambots and Decepticons*

Perhaps the most fundamental reason we are vulnerable to robots is that we trust them. Not only do we entrust them with our most intimate secrets and give them access to our most personal spaces, but we trust them with our physical well-being.[13] One of the fastest growing segments of robotics is in the field of health care.[14]

---

[11] *See* Benjamin Wittes & Jane Chong, *Our Cyborg Future: Law and Policy Implications*, BROOKINGS (September 2014), http://www.brookings.edu/research/reports2/2014/09/cyborg-future-law-policy-implications; *see also*, Ian Kerr, *The Internet of People? Reflections on the Future Regulation of Human-Implantable Radio Frequency Identification, in* PRIVACY, IDENTITY, AND ANONYMITY: LESSONS FROM THE IDENTITY TRAIL, (eds. Ian Kerr, Valerie Steeves and Carole Lucock, Oxford University Press, 2009).

[12] Maggie Hiufu Wong, *Bleep blorp: New Japanese hotel to be staffed by robots*, CNN (Feb. 5, 2015, 4:57), http://www.cnn.com/2015/02/04/travel/japan-hotel-robots/index.html.

[13] M. Ryan Calo, *Robots and privacy, in* ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS 187, 194 (Patrick Lin, Keith Abney & George A. Bekey ed. 2012).

[14] Laurel Riek, Woodrow Hartzog, Don Howard, AJung Moon, & Ryan Calo, The Emerging Policy and Ethics of Human Robot Interaction. In Proceedings of the 10th ACM/IEEE Conference on Human-Robot Interaction (HRI) (2015); see also, Sooyeon Jeong ET AL., *Deploying Social Robots in Pediatric Hospitals: What Needs to be Considered?,* The Emerging Policy and Ethics of Human Robot Interaction. In Proceedings of the 10th ACM/IEEE Conference on Human-Robot Interaction (HRI), 2015, http://www.openroboethics.org/hri15/wp-content/uploads/2015/02/Hf-Jeong-et-al.pdf; Heike Felzmann ET AL., *Robot-assisted Care for Elderly with Dementia: Is There a*

There are many reasons why people trust robots. Often the reason is that we have confidence in the manufacturer or designer because of their reputation. iRobot, a leader in the consumer robotics field and maker of the popular vacuum robot Roomba, enjoys a strong reputation among consumers.[15] Consumer trust in robots is also formed by company representations. In this way, robots are not unique. The FTC has a long history of protecting against deceptive representations by companies.

The FTC's most effective and commonly used regulatory tool is its authority to protect against deceptive trade practices in Section 5 of the FTC Act. A deceptive trade practice is any a material "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[16] According to the FTC:

> Practices that have been found . . . misleading or deceptive in specific cases include false oral or written representations, misleading price claims, sales of hazardous or systematically defective products or services without adequate disclosures, failure to disclose information regarding pyramid sales, use of bait and switch techniques, failure to perform promised services, and failure to meet warranty obligations.[17]

Rebecca Tushnet and Eric Goldman wrote "There are two pillars of truth in advertising according to the FTC: First, advertising must be truthful

---

Potential for Genuine End-user Empowerment?, The Emerging Policy and Ethics of Human Robot Interaction. In Proceedings of the 10th ACM/IEEE Conference on Human-Robot Interaction (HRI), 2015, http://www.openroboethics.org/hri15/wp-content/uploads/2015/02/Hf-Felzmann.pdf.

[15] *See e.g.*, Liam McCabe, *The Best Robot Vacuum*, THE SWEET HOME (Jan. 6, 2015), http://thesweethome.com/reviews/the-best-robot-vacuum-is-the-roomba-650/; *iRobot Roomba zooms past other robotic vacuums: But no robotic vacuum can replace your upright or canister*, CONSUMER REPORTS (Sept. 03, 2013, 2:00 PM), http://www.consumerreports.org/cro/news/2013/09/consumer-reports-tests-three-new-robotic-vacuums/index.htm.

[16] Letter from James C. Miller III to Hon. John D. Dingell, app. at 174–76 (1984); see also Letter from FTC Comm'rs to Wendell H. Ford & John C. Danforth, Senators (Dec. 17, 1980), reprinted in In re Int'l Harvester Co., 104 F.T.C. 949 app. at 1070–76 (1984), available at http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

[17] Letter from James C. Miller III to Hon. John D. Dingell, app. at 175.

and not misleading. Second, advertisers must have adequate substantiation for all product claims before disseminating their advertising."[18] The FTC has a long history of regulating deceptive advertising and marketing statements, including being on the forefront of niche and novel areas like blogger disclosure of benefits, subliminal advertising, drug advertising, negative-option marketing, and product demonstrations.[19] There are several scenarios emerging regarding the design and use of robots where the FTC might find deception.

Often there is a great difference between people's conceptions of what robots are currently able to do and what they are actually able to do. Society's notions of robots' capabilities are formed by popular movies, books and other aspects of pop culture and less by reality.[20] This makes marketing robots a ripe opportunity for deception because consumers are primed to believe.

For example, one of problematic kind of representation currently made by robotics companies has to do with "performance videos," often uploaded to a video sharing site or funding website like Kickstarter to tout a robot's features or effectiveness.[21] These videos sometimes speed up the motion of robots to make them appear faster than they are. In other instances, these videos simulate features that are planned, but might not yet exist. For example, the "Personal Robot" featured in a Kickstarter video by Robotbase simulates an advanced speech recognition that is aspirational and does not yet exist.[22]

---

[18] REBECCA TUSHNET & ERIC GOLDMAN, ADVERTISING AND MARKETING LAW 101 (2nd Edition 2014) (citing Advertising Substantiation Policy Statement, 49 Fed. Reg. 30999, Aug. 2, 1984).

[19] FTC DIVISION OF ADVERTISING PRACTICES, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-advertising-practices (last visited Mar. 17, 2015).

[20] *See* Neil M. Richards & William D. Smart, How Should the Law Think About Robots?, In Proceedings at We Robot 2012, University of Miami, http://robots.law.miami.edu/wp-content/uploads/2012/03/RichardsSmart_HowShouldTheLawThink.pdf.

[21] I thank Ryan Calo for bringing this problem to my attention.

[22] *See* Eamon Kunze, *Personal Robot Wants to be Your Ultimate Personal Assistant*, WT VOX (Feb. 20, 2015), https://wtvox.com/2015/02/personal-robot-wants-to-be-your-ultimate-personal-assistant/?utm_source=dlvr.it&utm_medium=twitter ("'The video is not an actual demonstration,' said CEO Duh Huynh. He told me it's a production video. 'It's what you'll get by the end of the year.' That's when Robotbase expects to start shipping

The FTC has an established track record regulating deceptive product demonstrations, which are forms of deceptive advertising.[23] For example, the FTC alleged that carmaker Volvo acted deceptively when making a commercial where all cars set for demolition in a monster truck show were crushed except a Volvo.[24] In reality, the Volvo's frame had been reinforced and the other cars' roof supports had been weakened.[25] The FTC also alleged that Campbell's Soup deceptively placed marbles at the bottom of a soup bowl in one of its ads to make soup appears as though it contained more vegetables than it really had.[26]

Another area of robotic deployment where deception becomes a problem involves what is known as a "Wizard-of-Oz setup."[27] According to Laurel Riek, "[Wizard of Oz] refers to a person…remotely operating a robot, controlling any of a number of things, such as its movement, navigation, speech, gestures, etc. [Wizard of Oz] may involve any amount of control along the autonomy spectrum, from fully autonomous to fully tele-operated, as well as mixed initiative interaction."[28] Jacqueline Kory Westlund and Cynthia Breazeal note that when a Wizard-of-Oz setup is deployed, "[a]t the most basic level, the human interacting with the remote-operated robot is deceived into thinking the robot is acting autonomously."[29]

---

the first of these personal robots to customers. When the robot does finally ship, Huynh admits that it's 'not going to have that sexy beautiful voice like in the video.'").

[23] *See, e.g.,* F.T.C. v. Colgate Palmolive, 380 U.S. 374 (1965) (sand on plexiglass used as a substitute for sand paper in a demonstration of shaving creme); S.C. Johnson & Son Inc. v. Clorox Co., 241 F.3d 232 (3d Cir. 2001) (rate of leakage from competitor's resealable bag was exaggerated) with See Nikkal Indus. Ltd. v. Salton, Inc., 735 F. Supp. 1227 (S.D.N.Y. 1990) (advertisement claiming scoopable ice cream was not deceptive despite a photograph of hard ice cream).

[24] Volvo N.A. Corp., 115 F.T.C. 87 (1992); Texas v. Volvo North America Corp., No. 493274 (Tex. D. Ct. Travis Co. 11/5/90) (depiction of a monster truck riding over cars in which a Volvo is not crushed was prosecuted because the roof supports of the Volvo had been reinforced and the other cars' roof supports have been weakened); *see also*

[25] *Id.*

[26] In re Campbell Soup Co., 77 F.T.C. 664 (1970).

[27] *See, e.g.,* Laurel D. Riek, Wizard of Oz Studies in HRI: A Systematic Review and New Reporting Guidelines, 1 Journal of Human-Robot Interaction 119 (2012).

[28] *Id.*

[29] Jacqueline Kory Westlund & Cynthia Breazeal, *Deception, Secrets, Children, and Robots: What's Acceptable?*, THE EMERGING POLICY AND ETHICS OF HUMAN ROBOT

Westlund and Breazeal noted some of the problems with the Wizard-of-Oz setup, where people "may disclose sensitive information to the robot that they would not tell a human, not realizing that a human is hearing everything they say. They may feel betrayed when they find out about the deception. Given that social robots are designed to draw us in, often engaging us emotionally and building relationships with us, the robot itself could be deceptive in that it appears to have an emotional response to you but 'in reality' does not."[30] When would a company's Wizard of Oz deployment become a deceptive trade practice? Given our general tendency to over-estimate the technological ability and agency of robots as social actors, the opportunity is ripe for malicious companies to scam users by convincing them they are dealing with a fully autonomous agent.

Riek and Robert Watson have also articulated how malicious actors might utilize security flaws in telepresence robots to deceive remote participants in a conversation.[31] Attackers could "modify messages, improperly obtain their contents, or prevent the system from operating at all."[32] With respect to video communications and telepresence, Riek and Watson find that telepresence manipulation can also be subtle, stating "modifications to the [communications] channel may not be immediately (or at all) obvious to the end user, as recent improvements in technology allow the realistic modification of both verbal and nonverbal communication signals in real

---

INTERACTION. In Proceedings of the 10th ACM/IEEE Conference on Human-Robot Interaction (HRI), 2015, http://www.openroboethics.org/hri15/wp-content/uploads/2015/02/Mf-Westlund.pdf.

[30] *Id.* (citing C.L. Breazeal, DESIGNING SOCIABLE ROBOTS (2004); M. Coeckelbergh, *Are Emotional Robots Deceptive?*, 3 IEEE TRANSACTIONS ON AFFECTIVE COMPUTING 388 (2012)); *see also*, David J. Atkinson, *Robot Trustworthiness: Guidelines for Simulated Emotion*, The Emerging Policy and Ethics of Human Robot Interaction. In Proceedings of the 10th ACM/IEEE Conference on Human-Robot Interaction (HRI), 2015, http://www.academia.edu/9889659/Robot_Trustworthiness_Guidelines_for_Simulated_Emotion.

[31] Laurel D. Riek & Robert N.M. Waton, *The Age of Avatar Realism: When Seeing Shouldn't Be Believing*, IEEE ROBOTICS & AUTOMATION MAGAZINE (December 2010), http://papers.laurelriek.org/riek-watson-final.pdf.

[32] *Id.*

time. This may allow the malicious modification of communication, or even the complete impersonation of a participant."[33]

Unlike inanimate objects, robots are capable of making their own representations. Some of these robots will inevitably deceive consumers. I will call lying robots "decepticons." Automated software 'bots' on social media like Twitter are increasingly adept at tricking people into thinking they are operated by humans.[34] Two of these bots were so convincing that when they "threatened" each other on Twitter, the police responded to their designer's house, confused about who actually "made" a death threat.[35] The same technology and techniques could also be employed in embodied robots.

Not all deception is actionable and not all decepticons are lawbreakers. A modest amount of inaccuracy is allowable, if not encouraged, under general principles of marketing and the messiness of human interaction. Many robots that end up misleading people might simply be engaged in trade puffery or common data analytics, similar to how a salesperson relies upon context and cues to tailor a strategy to best close the deal. Fortunately, as I will cover in Part II, the FTC has an established body of law to articulate the difference between deceptive and non-deceptive representations.

This jurisprudence will be important as robots become more involved in commerce. One of the core functions of the FTC is to protect consumers

---

[33] *Id.* ("[T]his kind of identity theft may be tricky to maintain because of the contextual information and subtle differences in…behavior, in particular, nonverbal behaviors that violate…expectations More subtly, [an attacker] might inject facial expressions and gestures into a conversation..[or]…may choose to inhibit…expressions, such as reducing the intensity of…smiles. [Attackers] can also augment or inhibit…tone of voice, or indeed even the words [said]. In the field of computer security, attacks such as these are referred to as a man-in-the-middle attack, in which a third party interferes with the expected execution of a protocol.").

[34] *See, e.g.* Nick Bilton, *Social Media Bots Offer Phony Friends and Real Profit*, N.Y. TIMES (Nov. 19, 2014), http://www.nytimes.com/2014/11/20/fashion/social-media-bots-offer-phony-friends-and-real-profit.html.

[35] *See* Lee Mathews, *Police respond to Twitter bot sending death threat to another Twitter bot*, GEEK (Feb. 11, 2015, 1:29 PM), http://www.geek.com/apps/police-respond-to-twitter-bot-sending-death-threat-to-another-twitter-bot-1615550/.

against scams.[36] In addition to the agency's focus on claims that can affect health and physical well-being, the FTC dedicates much of its resources to fighting those who target financially vulnerable consumers or economically harm consumers.[37]

It is worth noting that the relatively new Consumer Financial Protection Bureau (CFPB) arguably has even more authority over scammers than the FTC. The CFPB can regulate "abusive" conduct as well as "unfair" conduct.[38] An "abusive" practice is one that:

> (1) materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service; or
>
> (2) takes unreasonable advantage of—
>
> (A) a lack of understanding on the part of the consumer of the material risks, costs, or conditions of the product or service;
>
> (B) the inability of the consumer to protect the interests of the consumer in selecting or using a consumer financial product or service; or
>
> (C) the reasonable reliance by the consumer on a covered person to act in the interests of the consumer.[39]

Because of its ability to regulate abusive conduct, the CFPB might be even more empowered than the FTC to regulate those that would exploit irrational consumer biases such as our tendency to attribute agency to robots, form emotion bonds to them, and irrationally trust the results of

---

[36] Scam Alerts: What To Know and Do About Scams in the News, FTC, http://www.consumer.ftc.gov/scam-alerts (last accessed March 19, 2015).
[37] REBECCA TUSHNET & ERIC GOLDMAN, ADVERTISING AND MARKETING LAW 101 (2nd Edition 2014).
[38] Consumer Financial Protection Act § 1031(d)(2); *see also* REBECCA TUSHNET & ERIC GOLDMAN, ADVERTISING AND MARKETING LAW 115 (2nd Edition 2014).
[39] *Id.*

automated decisions.[40] As I'll argue in detail below, it will take many agencies to effectively address consumer robotics. And scambots are not the only robots that might pose problems for consumers.

2. *Spybots*

Robots will eventually assist consumers in both banal and intimate aspects of people's lives. To be effective, robots must sense the world around them. Robots have been equipped with cameras, motion and audio sensors, facial and object recognition technologies, and even biological sensors that measure pulse, pupil dilation, and hair follicle stimulation.[41] They have the capacity to store massive quantities of personal data in perfect, easily recalled form. When robots are fully realized, they will be nothing short of a perfected surveillance machine. [42]

Ryan Calo has argued that robots introduce new points of access to historically protected spaces.[43] Calo noted, "The home robot in particular presents a novel opportunity for government, private litigants, and hackers to access information about the interior of a living space."[44]

Spybots are also particularly problematic because people give robots social meaning.[45] Calo stated, "Robots are increasingly human-like and

---

[40] *See* generally Benedict J. Schweigert, The CFPB's "Abusiveness" Standard and Consumer Irrationality, SSRN (May 15, 2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2061733.

[41] M. Ryan Calo, *Robots and Privacy, in* ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS 187, 194 (Patrick Lin, Keith Abney & George A. Bekey ed. 2012); Kristen Thomasen, Liar Liar Pants on Fire! Examining the Constitutionality of Enhanced Robo-Interrogation, In Proceedings of We Robot Conference, University of Miami, 2012, http://robots.law.miami.edu/program/%3Ca%20href=; Adam Higgenbotham, Deception is Futile When Big Brother's Lie Detector Turns Its Eyes on You, WIRED (Jan. 17, 2013), http://www.wired.com/2013/01/ff-lie-detector/.

[42] M. Ryan Calo, *Robots and Privacy, in* ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS 187, 194 (Patrick Lin, Keith Abney & George A. Bekey ed. 2012). ("It is not hard to imagine why robots raise privacy concerns…Robots can go places humans cannot go, see things humans cannot see. Robots are, first and foremost, a human instrument. And, after industrial manufacturing, the principle use to which we've put that instrument has been surveillance.").

[43] *Id.* at 188.

[44] *Id.*

[45] *Id.*

socially interactive in design, making them more engaging and salient to their end-users and the larger community. Many studies demonstrate that people are hardwired to react to heavily anthropomorphic technologies, such as robots, as though a person were actually present, including with respect to the sensation of being observed and evaluated."[46]

Calo argued that the social dimension of robots opens up three distinct dangers: humans will have fewer opportunities for solitude, robots will be in a unique position to extract information from people, and robots can leverage the advantages of humans (such as fear and praise) in information gathering without human drawbacks such as imperfect memories, fatigue, and embarrassment.[47]

Spybots are already so prevalent that it is impractical to try to describe all of the different types. Drones have ignited America's peeping tom anxiety and they are getting smaller by the day.[48] One company has marketed "Nixie," a small robot that looks like a watch with propellers, as the first wearable camera that can fly.[49] Visions of drone-covered skies and hidden drones peeping into bedrooms easily trigger consumer distaste for surveillance. Some of these drones might be regulated under the same theories that the FTC has used to regulate spyware.[50]

---

[46] *Id.*

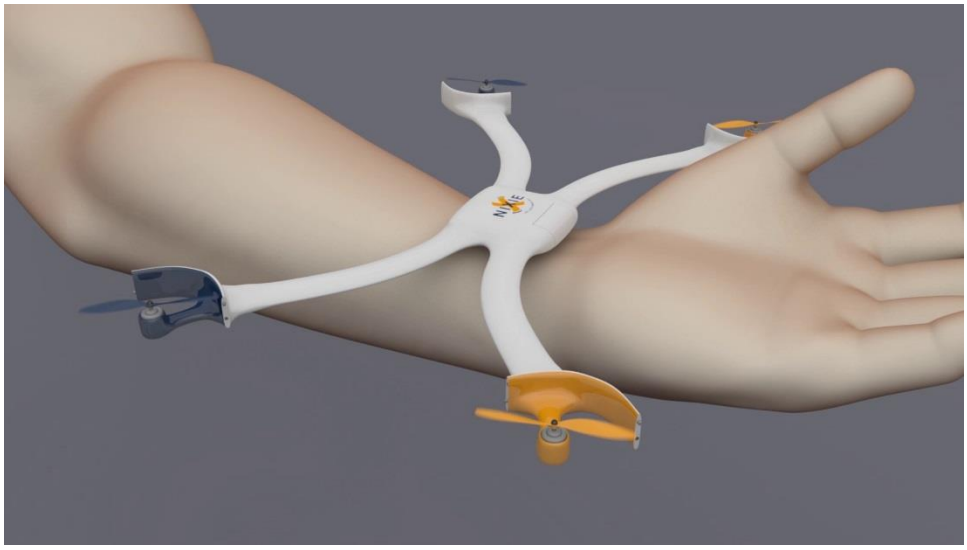
[47] *Id.*

[48] *See e.g.*, Ryan Calo, *The Drone as Privacy Catalyst*, 64 STAN. L. REV. ONLINE 2 (2011); Gregory S. McNeal, Alleged Drone 'Peeping Tom' Photo Reveals Perils of Drone Related Journalism, Forbes (Jul. 14, 2014, 4:14 PM), http://www.forbes.com/sites/gregorymcneal/2014/07/14/alleged-drone-peeping-tom-photo-reveals-perils-of-drone-related-journalism/ ; Erica Heartquist, *Drone Accused of Peeping into Woman's Window Was Photographing Aerial Views*, USA TODAY (Jun. 24, 2014, 10:40 PM EDT), http://www.usatoday.com/story/news/nation-now/2014/06/24/seattle-woman-drone-apartment-washington/11339835/.

[49] NIXIE, http://flynixie.com/ (last visited Mar. 17, 2015).

[50] *See, e.g.,* In re Aspen Way Enters., Inc., FTC File No. 112 3151, No. C-4392 (F.T.C. Apr. 11, 2013); In re CyberSpy Software, LLC and Trace R. Spence, FTC File No. 082 3160, No. 08-CV-01872 (F.T.C. Nov. 17, 2008) (alleging that selling spyware and showing customers how to remotely install it on other people's computers without their knowledge or consent is an unfair and deceptive trade practice);.*see also* Spyware and Malware, FTC, https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security/spyware-and-malware; In re CyberSpy Software, LLC and Trace R. Spence, FTC File No. 082 3160, No. 08-CV-01872 (F.T.C. Nov. 17, 2008).

Figure 1: Nixie, the Wearable Camera Drone



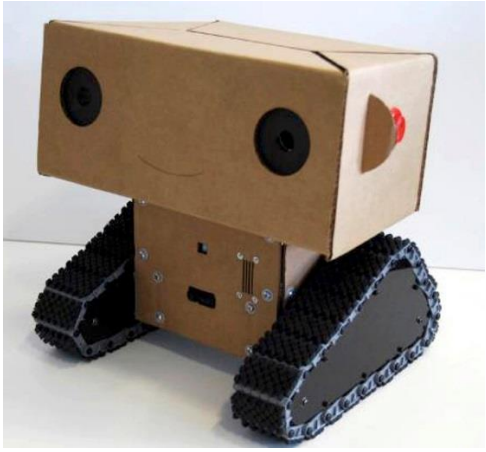
The FTC has alleged that the sale of spyware, as well as providing the means and instrumentalities to install spyware and access consumer's personal information, are unfair and deceptive trade practices.[51] The FTC has also concluded that installing spyware and gathering data without notice was an unfair practice.[52] The FTC has deemed the surreptitious data gathering unfair. The agency cited to the substantial harm caused to consumers from such invasive surveillance and concerns that "[c]onsumers cannot reasonably avoid these injuries because [the surveillance] is invisible to them."[53] The FTC filed an unfairness complaint against Sony BMG on a similar theory alleging that the company caused spyware to be downloaded without sufficient notice.[54] When is robotic surveillance like spyware? When it is not obvious? When it is undetectable?

---

[51] *See, e.g.,* In re CyberSpy Software, LLC and Trace R. Spence, FTC File No. 082 3160, No. 08-CV-01872 (F.T.C. Nov. 17, 2008).
[52] In re Aspen Way Enters., Inc., FTC File No. 112 3151, No. C-4392 (F.T.C. Apr. 11, 2013).
[53] *Id.*
[54] In re Sony BMG Music Entm't, FTC File No. 062 3019, No. C-4195 (F.T.C. June 28, 2007), available at http://www.ftc.gov/sites/default/files/documents/cases/2007/01/070130cmp0623019.pdf.

Boxie, an interactive story-capture robot developed at MIT, demonstrates how people will give a random robot unquestioned access and personal information simply because it is adorable and unthreatening.[55] Boxie was designed specifically to coax stories out of people and succeeded in that goal.

Figure 2. Boxie, the Painfully Cute Information-Extractor



Consider how robots like Boxie might be deployed as a robot shopping assistant. Robotic shopping assistants, which are currently deployed in Japan, are designed to approach customers and encourage the purchase

---

[55] BOXIE: THE INTERACTIVE STORY-CAPTURE CAMERA, http://resenv.media.mit.edu/Boxie/ (last visited Mar. 17, 2015); *see also*, Kasia Cieplak-Mayr von Baldegg, *The World's Cutest Surveillance Robot Videographer*, THE ATLANTIC (Jan. 13, 2012, 10:32 AM ET), http://www.theatlantic.com/video/archive/2012/01/the-worlds-cutest-surveillance-robot-videographer/251370/; Paul Marks, *Robot Videojournalist Uses Cuteness to Get Vox Pops*, NEW SCIENTIST (Dec. 28, 2011, 13:57), http://www.newscientist.com/article/dn21318-robot-videojournalist-uses-cuteness-to-get-vox-pops.html#.VQb9j47F93E.; *see also* Laura Sydell, SXSW Debuts Robot Petting Zoo For A Personal Peek Into The Future, NPR's All Tech Considered (Mar. 18, 2015), http://www.npr.org/blogs/alltechconsidered/2015/03/18/393614456/sxsw-debuts-robot-petting-zoo-for-a-personal-peek-into-the-future ("BlabDroid actually has some pretty sophisticated wiring inside, but with its cardboard shell with a smile cut into it, he looks like he was made in someone's garage. [The robot's creator] says that's intentional. "In a relationship with a robot, where you're being very vulnerable, the other actor in that situation has to be as vulnerable as you," he says. "So if the robot is small, tiny, made out of cardboard, you kind of feel like you can open up to him more because he's very familiar and you feel like you're in control of that situation.").

of a particular product or service. Calo has noted "Unlike ordinary store clerks, however, robots ae capable of recording and processing every aspect of the transaction. Face-recognition technology permits easy re-identification. Such meticulous, point-blank customer data could be of extraordinary use in both loss prevention and marketing research."[56] Given this kind of utility, such features on robots of all kinds seem likely. Like the ubiquity of smartphones, we will be surrounded by mechanical watchers.[57]

While the FTC does not have a long history of regulating surveillance technologies, over the past twenty years it has begun to develop a theory of unfair and deceptive surveillance and information gathering. For example, the FTC has charged a number of companies with deceptive trade practices for creating a deceptively fake software "registration" page to obtain personal information from technology users.[58] Because only

---

[56] M. Ryan Calo, *Robots and Privacy, in* ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS 190 (Patrick Lin, Keith Abney & George A. Bekey ed. 2012)

[57] *See* Bruce Schneier, *Cell Phone Spying*, SCHNEIER ON SECURITY BLOG (May 9, 2008, 6:27 AM), https://www.schneier.com/blog/archives/2008/05/cell_phone_spyi_1.html; *see also*, Bruce Schneier, *Tracking People from Smartphone Accelerometers*, SCHNEIER ON SECURITY BLOG (April 30, 2014, 1:05 PM), https://www.schneier.com/blog/archives/2014/04/tracking_people_2.html.

[58] A number of FTC actions have centered on the creation and use of fake registration spyware software called "Detective Mode." E.g., Complaint at 5, In re DesignerWare, LLC, FTC File No. 112 3151, No. C-4390 (F.T.C. Apr. 11, 2013) [hereinafter DesignerWare Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwarecmpt.pdf (charging company that created and licensed "Detective Mode"). For examples of companies charged with using Detective Mode to improperly gather personal information on users, see Complaint at 2, In re Aspen Way Enters., Inc., FTC File No. 112 3151, No. C-4392 (F.T.C. Apr. 11, 2013) [hereinafter Aspen Way Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415aspenwaycmpt.pdf; Complaint at 3, In re B. Stamper Enters., Inc., FTC File No. 112 3151, No. C-4393 (F.T.C. Apr. 11, 2013), available at http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415bstampercmpt.pdf; Complaint at 3, In re C.A.L.M. Ventures, Inc., FTC File No. 112 3151, No. C-4394 (F.T.C. Apr. 11, 2013), available at http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415calmcmpt.pdf; Complaint at 3, In re J.A.G. Rents, LLC, FTC File No. 112 3151, No. C-4395 (F.T.C. Apr. 11, 2013), available at http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415jagcmpt.pdf; Complaint at 3, In re Red Zone Inv. Grp., Inc., FTC File No. 112 3151, No. C-4396 (F.T.C.

some types of surveillance were disclosed to the user, the FTC asserted the companies acted deceptively when they failed to tell users the nature of the questions they were being asked via software. [59]

In *FTC v. Frostwire, LLC*, the FTC alleged that a software company deceived consumers through its user interface when it failed to notify consumers adequately regarding how its file-sharing software operated, including the fact that downloaded files were shared publicly by default as well as the fact that the software "would publicly share files that consumers previously downloaded…and stored in 'unshared' folders even after consumers deselected the Share Finished Downloads setting in the Options-Sharing dialog box."[60]

Should robot designers and users also be obligated disclose to consumers how their personal information is being collected? Or should users simply always be aware that when they are interacting with a robot that their personal information is fair game? Does it matter that robots like Boxie are specifically designed to extract personal information through social engineering?

Apr. 11, 2013), available at http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415redzonecmpt.pdf; Complaint at 2, In re Watershed Dev. Corp., FTC File No. 112 3151, No. C-4398 (F.T.C. Apr. 11, 2013), available at http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415watershedcmpt.pdf; see also Compete Complaint, supra note 217, at 2–3 (charging company for improperly tracking customers' internet use)

[59] See, e.g., Complaint at 2, In re Epic Marketplace, Inc., FTC File No. 112 3182, No. C-4389 (F.T.C. Mar. 13, 2013) [hereinafter Epic Marketplace Complaint], available at http://www.ftc.gov/sites/default/files/documents/cases/2013/03/130315epicmarketplacecmpt.pdf (charging company for failing to disclose "history sniffing" practice). For an explanation of a deceptive omission, see Letter from James C. Miller III to Hon. John D. Dingell, supra note 42, app. at 175 n.4 ("A misleading omission occurs when qualifying information necessary to prevent a practice, claim, representation, or reasonable expectation or belief from being misleading is not disclosed. Not all omissions are deceptive, even if providing the information would benefit consumers.").

[60] Complaint for Permanent Injunction and Other Equitable Relief at 19, FTC v. Frostwire, LLC, No. 1:11-cv-23643 (S.D. Fla. Oct. 12, 2011), available at http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111011frostwirecmpt.pdf.

Surveillance is not the only problematic method of collecting personal information. The FTC also views the act of "pretexting" to be a generally deceptive practice when used to obtain personal information. According to the FTC, pretexting involves "making various misleading and false statements to financial institutions and others. Such tactics include calling financial institutions and pretending to be the account holder, thereby inducing the financial institution to disclose private financial information," and, upon obtaining this private information, selling it.[61]

Telepresence manipulation could be a form of pretexting. Would using a Wizard-of-Oz setup to obtain information be considered similar to pretexting, given that the fundamental culpability in pretexting lies in the fact that information was obtained by a person pretending to be someone (or something) more likely to be entrusted with personal information?

3. *Nudgebots*

We humans are a persuadable bunch. Over the last half-century, mounting evidence demonstrates that humans are subject to numerous biases that motivate us to act in predictably irrational ways.[62] Humans rely too heavily on available anecdotes and judgments reached by computers.[63] We attribute human emotions and agency to machines.[64] We care too much what others think about us and we increasingly entrench ourselves in opinions formed based on trivial, anecdotal, and arbitrary

---

[61] Complaint for Injunction and Other Equitable Relief, FTC v. Rapp, No. 99-WM-783 (D. Colo. Apr. 21, 1999), available at http://www.ftc.gov/sites/default/files/documents/cases/1999/04/ftc.gov-touchtonecomplaint.htm.

[62] *See, e.g.,* DANIEL KAHNEMAN, THINKING FAST AND SLOW (2013); DAN ARIELY, PREDICTABLY IRRATIONAL: THE HIDDEN FORCES THAT SHAPE OUR DECISIONS (2d ed. 2009); DANIEL THAYER & CASS SUNSTEIN, NUDGE: IMPROVISING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2d ed. 2009).

[63] *See* DANIEL KAHNEMAN, THINKING, FAST AND SLOW (2013); Daniel Keats Citron, Technological Due Process, 85 WASH. U. L. REV. 1249 (2007).

[64] *See* Kate Darling, *Extending Legal Rights to Social Robots*. In Proceedings of We Robot Conference, University of Miami, 2012, http://robots.law.miami.edu/wp-content/uploads/2012/03/Darling_Extending-Legal-Rights-to-Social-Robots.pdf

evidence.[65] Even worse, we consistently fall prey to these biases. This fact is well known and regularly exploited.

Our vulnerability to manipulation combined with the technical and social power of robots could create more problems for consumers. One of the most interesting questions is the extent to which robots will be allowed to "nudge" humans. Cass Sunstien, who helped develop the concept of nudging, defines nudges as "liberty-preserving approaches that steer people in particular directions, but that also allow them to go their own way."[66]

Nudging can be acceptable, if not inevitable, in many circumstances. But it is not always clear at what point nudging turns to wrongful manipulation. Ryan Calo has developed a theory of digital market manipulation that pinpoints three problematic contexts where personal information is leveraged to manipulate consumers: the mass production of bias, disclosure ratcheting, and means-based targeting.[67] A theory of wrongful robotic manipulation of consumers could be useful. Consider the different techniques my hypothetical "Boxie the Shopping Assistant" might use to encourage sales. What if Boxie was part of a Wizard-of-Oz setup? Should companies be required to disclose their robots are not fully autonomous?

The FTC has a long history of regulating high-pressure sales techniques and otherwise wrongful sales tactics. For example, the agency has recently targeted negative-option marketing, in which "sellers interpret a customer's failure to take an affirmative action, either to reject an offer or cancel an agreement, as assent to be charged for goods or services."[68]

---

[65] DANIEL KAHNEMAN, THINKING FAST AND SLOW (2013); DAN ARIELY, PREDICTABLY IRRATIONAL: THE HIDDEN FORCES THAT SHAPE OUR DECISIONS (2d ed. 2009); DANIEL THAYER & CASS SUNSTEIN, NUDGE: IMPROVISING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2d ed. 2009).

[66] DANIEL THAYER & CASS SUNSTEIN, NUDGE: IMPROVISING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2d ed. 2009); Cass Sunstein, *Nudging: A Very Short Guide*, available on SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2499658.

[67] Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014).

[68] Negative Options: A Report by the Staff of the FTC's Division of Enforcement, FTC (January 2009), https://www.ftc.gov/sites/default/files/documents/reports/negative-options-federal-trade-commission-workshop-analyzing-negative-option-marketing-report-staff/p064202negativeoptionreport.pdf; *see also* FTC v. Willms, No. 2:11-cv-

Negative option tactics take advantage of people's noted bias for the status quo.[69]

In the past, the FTC has categorized manipulative sales tactics as an unfair trade practice.[70] In its statement on unfairness, the FTC articulated a few boundaries for manipulation, stating "certain types of sales techniques may prevent consumers from effectively making their own decisions, and that corrective action may then become necessary."[71] The FTC stated that these actions are brought "not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking."[72]

The goal of the FTC in this space is to keep companies from hindering free market decisions. Examples of wrongful tactics include withholding or failing to generate an important price or performance information, "for example, leaving buyers with insufficient information for informed comparisons. Some [sellers] may engage in overt coercion, as by dismantling a home appliance for "inspection" and refusing to reassemble it until a service contract is signed. And some may exercise undue influence over highly susceptible classes of purchasers, as by promoting fraudulent 'cures' to seriously ill cancer patients."[73] According to the FTC, "Each of these practices undermines an essential precondition to a free

---

00828-MJP (W.D. Wash. Mar. 6, 2012) (stipulated final judgment and order); see also 16 C.F.R § 425 (2014) (imposing requirements on negative option marketing).

[69] See, e.g., Cass R. Sunstein, Impersonal Default Rules vs. Active Choices vs. Personalized Default Rules: A Triptych 9 (May 19, 2013) (unpublished manuscript), available at http://ssrn.com/abstract_id=2171343 ("In the domain of privacy on the Internet, a great deal depends on the default rule.").

[70] *See* Holland Furnace Co. v. ETC, 295 F.2d 302 (7th Cir. 1961); *cf* Arthur Murray Studio, Inc. v. EW, 458 F.2d 622 (5th Cir. 1972) (emotional high-pressure sales tactics, using teams of salesmen who refused to let the customer leave the room until a contract was signed); *see also* Statement of Basis and Purpose, Cooling-Off Period for Door-to-Door Sales, 37 Fed. Reg. 22934, 22937-38 (1972).

[71] FTC Policy Statement on Unfairness, Letter from FTC Comm'rs to Wendell H. Ford & John C. Danforth, Senators (Dec. 17, 1980), reprinted in In re Int'l Harvester Co., 104 F.T.C. 949 app. at 1070–76 (1984), available at http://www.ftc.gov/bcp/policystmt/ad-unfair.htm (explaining evolution of, and rationale for, FTC's consumer unfairness jurisdiction).

[72] *Id.*

[73] *Id.*

and informed consumer transaction, and, in turn, to a well-functioning market. Each of them is therefore properly banned as an unfair practice under the FTC Act."[74]

Robots, particularly embodied ones, are uniquely situated to mentally manipulate people. Robots can mimic human socialization, yet they are without shame, fatigue, or internal inconsistency. Robots are also scalable, so the decision to design a robot to manipulate humans will impact hundreds, if not thousands or millions of people.

Nudgebots are already at work in society. Tinder, the social dating mobile app, has recently been flooded with bots posing as actual users attempting to persuade users to download apps.[75] The bots will pose as actual users by using typical Tinder conversational language such as "Hey :)," "What're you doing?" and "I'm still recovering from last night :) Relaxing with a game on my phone, castle cash. Have you heard of it?"[76]

If the user replies at all, the bot will send the user a link with a trustworthy-sounding address www.tinderverified.com/ along with a message telling to user to "play with me a bit and you just might get a phone number."[77] Another sophisticated bot on Tinder tricks users into disclosing credit card numbers as an elaborate scheme to "verify" a webcam service under the guise of an invitation to engage in online foreplay.[78] As if dating was not complicated enough already.

Of all areas where the FTC might regulate robotics, nudgebots seem the murkiest. While deception might be relatively easy to spot in some instances, other equally harmful tactics, such as exploitation of emotional attachment to make a sale, might be more difficult to spot and even

---

[74] *Id.*
[75] Leo Kelion, Tinder accounts spammed by bots masquerading as singles, BBC (Apr. 2, 2014), http://www.bbc.com/news/26850761.
[76] *Id.*
[77] *Id.*
[78] Satnam Nurang, Tinder: Spammers Flirt with Popular Mobile Dating App, SYMANTEC (Jul. 1, 2013), http://www.symantec.com/connect/blogs/tinder-spammers-flirt-popular-mobile-dating-app?SID=skim38395X1020946X4058df191d7e8584f3eb6715dacc5ed7&API1=100&API2=7104284.

harder to articulate a consistent framework for regulating. Catfishing aside, all people play roles when they are interacting with others.[79]

But at some point, it seems clear that our tendency to emotionally invest in robots is a vulnerability worth regulatory attention. Kate Darling has examined one possible approach: the law might protect robots.[80] Among other reasons, Darling suggests we might want to protect robots because of the effect robot harm has on humans. Darling has cataloged the human tendency to form emotional bonds with robots and over-ascribe them with agency, intelligence, emotion, and feeling. She noted:

> [W]hen the United States military began testing a robot that defused landmines by stepping on them, the colonel in command called off the exercise. The robot was modeled after a stick insect with six legs. Every time it stepped on a mine, it lost one of its legs and continued on the remaining ones. According to Garreau (2007), "[t]he colonel just could not stand the pathos of watching the burned, scarred and crippled machine drag itself forward on its last leg. This test, he charged, was inhumane."
>
> Other autonomous robots employed within military teams evoke fondness and loyalty in their human teammates, who identify with the robots enough to name them, award them battlefield promotions and "purple hearts", introduce them to their families, and become very upset when they "die." While none of these robots are designed to give emotional cues, their autonomous behavior makes them appear lifelike enough to generate an emotional response. In fact, even simple household robots like the Roomba vacuum cleaner prompt people to talk to

[79] *See, e.g.,* Erving Goffman, The Presentation of Self in Everyday Life (1959).
[80] Kate Darling, Extending Legal Rights to Social Robots, In Proceedings of We Robot 2012, University of Miami, http://robots.law.miami.edu/wp-content/uploads/2012/04/Darling_Extending-Legal-Rights-to-Social-Robots-v2.pdf.

> them and develop feelings of camaraderie and gratitude[81]

Ryan Calo similarly notes, "There is an extensive literature to support the claim that people are "hardwired" to react to anthropomorphic technology such as robots as though a person were actually present. The tendency is so strong that soldiers have reportedly risked their own lives to 'save' a military robot in the field."[82]

My family owns a Roomba. We named it "Rocco." Let's say I buy a future version of this useful technology from a less scrupulous robotics company than iRobot. Our new version of Rocco is anthropomorphized and outfitted with a cute face, voice, and personality. Assume new Anthro-Rocco dutifully serves my family for years. It asks us how we're feeling, tells us jokes like how much its job "sucks," and over time our family becomes quite attached to Rocco. One day poor Rocco starts to sputter along as though sick, looks up at me with its round, cute eyes, and says "Daddy…[cough]…if you don't buy me a new software upgrade…I'll die."

I hope I'll be able to resist this super-charged Tamagotchi's underhanded sales technique.[83] But will all consumers be able to resist Rocco's charm? How might robots like these affect the elderly, for whom robots have great potential as companions?[84] Or what about children, who have difficulty parsing complex emotional attachments and understanding how robots work. Research demonstrates that children can think of robots as a social being and a friend.[85] Children tell robots secrets that they do not trust

---

[81] *Id.*

[82] Ryan Calo, The Case for a Federal Robotics Commission, Brookings (September 2014), http://www.brookings.edu/research/reports2/2014/09/case-for-federal-robotics-commission (citing P.W. Singer, Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century 337-43 (2009)).

[83] Tamagotchi, WIKIPEDIA, http://en.wikipedia.org/wiki/Tamagotchi (last visited Mar. 18, 2015).

[84] A Robotics Companion for the Elderly?, GE IDEA LAB (Aug. 13, 2014), http://www.ideaslaboratory.com/post/94619189589/a-robotic-companion-for-the-elderly; *but see* Amanda Sharkey and Noel Sharkey, *Granny and the Robots: Ethical Issues in Robot Care for the Elderly*, 14 ETHICS AND INFORMATION TECHNOLOGY 27 (2012), http://link.springer.com/article/10.1007/s10676-010-9234-6/fulltext.html.

[85] Jacqueline Kory Westlund & Cynthia Breazeal, *Deception, Secrets, Children, and Robots: What's Acceptable?*, THE EMERGING POLICY AND ETHICS OF HUMAN ROBOT INTERACTION. In Proceedings of the 10th ACM/IEEE Conference on Human-Robot

with adults.[86] Of course, children also tell secrets to stuffed animals, but mere stuffed animals cannot programed to extract information or fake emotional bonds via a Wizard-of-Oz setup.

The FTC is acutely sensitive to manipulation of vulnerable populations. Entire regimes, such as the Children's Online Privacy Protection Act, are designed to protect children, who are generally less aware of risk and therefore less able to avoid it.[87] The elderly are particularly vulnerable to fraud and are common scam targets and victims.[88] There is little reason to think this will change with the mass adoption of consumer robotics. Thus the FTC should begin to address how its existing jurisprudence on deception and manipulation will apply to nudgebots.

4. Autobots

Whether algorithms and software, by themselves, are properly classifiable as "robots" is debatable.[89] However, algorithms enable automation, which is a signature trait of robotics. Thus, they are worthy of consideration along with other consumer robotics issues. Frank Pasquale has noted the incredible power of algorithms, stating "Decisions that used to be based on human reflection are now made automatically. Software encodes thousands of rules and instructions computed in a fraction of a second."[90] Algorithms are the instructions that dictate how a robot will operate. Thus, they are consequential and present consumer protection issues.

Interaction (HRI), 2015, http://www.openroboethics.org/hri15/wp-content/uploads/2015/02/Mf-Westlund.pdf.

[86] *Id.*

[87] Children's Online Privacy Protection Rule, FTC, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule (last accessed Mar. 19 2015).

[88] FTC Testifies on Fraud Against Older Americans, FTC (May 16, 2013), https://www.ftc.gov/news-events/press-releases/2013/05/ftc-testifies-fraud-against-older-americans.

[89] *See, e.g.*, Neil M. Richards & William D. Smart, How Should the Law Think About Robots?, In Proceedings at We Robot 2012, University of Miami, http://robots.law.miami.edu/wp-content/uploads/2012/03/RichardsSmart_HowShouldTheLawThink.pdf.

[90] FRANK PASQUALE, BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 8 (2015).

Pasquale notes that algorithms are endemic in reputation, search, and finance, yet they are shrouded in secrecy.[91] According to Pasquale, "The values and prerogatives that the encoded rules enact are hidden within black boxes. The most obvious question is: Are these algorithmic applications fair?"[92] Pasquale and Danielle Citron have warned of a "scored society," where much of people's lives and reputations are quantified and ranked.[93] Solon Barocas and Andrew Selbst have noted the potential for algorithms and big data to have a disparate impact on vulnerable and minority populations.[94]

David Vladeck has argued that "society will need to consider whether existing liability rules will be up to the task of assigning responsibility for any wrongful acts [fully autonomous robots] commit."[95] According to Vladeck, "The first generation of fully autonomous machines--perhaps driver-less cars and fully independent drone aircraft--will have the capacity to act completely autonomously. They will not be tools used by humans; they will be machines deployed by humans that will act independently of direct human instruction, based on information the machine itself acquires and analyzes, and will often make highly consequential decisions in circumstances that may not be anticipated by, let alone directly addressed by, the machine's creators."[96]

Vladeck argued that the key question for autonomous thinking machines "is whether it is fair to think of them as agents of some other individual or entity, or whether the legal system will need to decide liability issues on a basis other than agency."[97] Vladeck proposed several possible direct, indirect, and shared liability answers to this question, including strict and

---

[91] *Id.*
[92] *Id.* 8-9.
[93] Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014).
[94] Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. (forthcoming 2016), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899.
[95] David C. Vladeck, *Machines Without Principals: Liability Rules and Artificial Intelligence*, 89 WASH. L. REV. 117, 121 (2014).
[96] *Id.*
[97] *Id.* at 122.

"common enterprise" liability, or even the possibility of suing the robot itself under a theory of "conferred personhood."[98]

This article will not engage the plentiful literature on the consumer benefits and problems created by algorithms and the automation of robots.[99] Many issues involving algorithms are related to broader public policies and issues of social justice, which are harder to obtain solely through Section 5 of the FTC Act. It is enough to note that algorithms and automation now present consumer protection issues. The FTC has already started to take notice of algorithms in related contexts, such as privacy. FTC Chief Technologist Ashkan Soltani has put algorithmic transparency on his agenda for his tenure at the agency, stating "I hope to expand the agency's ability to measure big data's disparate effects in order to ensure that the algorithms that consumers interact with on a daily basis afford them the same rights online as they're entitled to offline."[100]

Machine learning issues aside, robots will do as they are told, so we must be very careful with what we tell them.[101] Many of the issues presented by algorithms will be part of a larger, problematic kind of robot. For example, a nudgebot designed to exploit a person's vulnerability is running a malicious algorithm. Yet algorithms might also be worth consideration on their own merit, particularly with respect to possible remedies.

As will be discussed below, the FTC has several tools including disclosures and design requirements that could ameliorate the harms from secret algorithms. Can algorithms be so complex that meaningful transparency is impossible? Is it enough to modify only algorithms if the rest of a robots design, such as its external features and physical manipulation capabilities, remain capable of harm? Does it matter if robots can engage in machine learning as a form of artificial intelligence? What is the culpability of humans operating robots if they do not understand the content or effect of a robot's algorithms?

---

[98] *Id.* at 145-150.
[99] *See, e.g.*, NICK CARR, THE GLASS CAGE: AUTOMATION AND US (2014).
[100] Ashkan Soltani, Hello World!, FTC (Dec. 2, 2014), https://www.ftc.gov/news-events/blogs/techftc/2014/12/hello-world.
[101] With apologies to Kurt Vonnegut, Jr.

5. *Cyborgs*

The final consumer robotics concern that the FTC will need to address is when people actually become robots, at least partially. Becoming a true cyborg in the classic sci-fi sense may still be some time away. Yet in many ways the science and reality of man-machine hybrids is closer than you think.[102] Exoskeletons hold the promise of mobility. Some have argued mobile phones are so integral to our person that we should already consider ourselves cyborgs.[103]

But one of the main immediate issues of concern involves the physical implanting of technology into people's bodies. Benjamin Wittes and Jane Chong write, "whether or not a technology can be considered medically superficial in function, once we incorporate it into the body such that it is no longer easily removed, it is integral to the person in fact. A number of bars, strip clubs and casinos have banned the use of Google Glass based on privacy protection concerns, and movie theaters have banned it for reasons related to copyright protection. But such bans could pose problems when the equivalent of Google Glass is physically screwed into an individual's head."[104]

Implantables are not a fantasy. Neil Harbisson, a cyborg activist had an "eyeborg" device that allows him to "hear" color installed in his head.[105] After robots, the next "Internet of Things" will likely be the "Internet of Things Inside Our Body."[106] RFID tags are currently implantable, and raise considerable ethical and legal issues, including privacy and

---

[102] Benjamin Wittes & Jane Chong, *Our Cyborg Future: Law and Policy Implications* BROOKINGS (September 2014), http://www.brookings.edu/research/reports2/2014/09/cyborg-future-law-policy-implications.

[103] *Id.*

[104] *Id.*

[105] Benjamin Wittes & Jane Chong, *Our Cyborg Future: Law and Policy Implications* BROOKINGS (September 2014), http://www.brookings.edu/research/reports2/2014/09/cyborg-future-law-policy-implications.

[106] Ian Kerr, *The Internet of People? Reflections on the Future Regulation of Human-Implantable Radio Frequency Identification*, IN PRIVACY, IDENTITY, AND ANONYMITY: LESSONS FROM THE IDENTITY TRAIL, (eds. Ian Kerr, Valerie Steeves and Carole Lucock, Oxford University Press, 2009).

autonomy, the limits of implanted software licensing, and health and safety issues.[107] This is to say nothing of the promise and associated problems with nanotechnology.[108]

Perhaps of most immediate concern to the FTC is the security of data on implantable devices.[109] Wittes and Chong write:

> As it turns out, the state of the law with respect to pacemakers and other implanted medical devices provides a particularly vivid illustration of a cyborg gap. Most pacemakers and defibrillators are outfitted with wireless capabilities that communicate with home transmitters that then send the data to the patient's physician. Experts have demonstrated the existence of enormous vulnerabilities in these software-controlled, Internet-connected medical devices, but the government has failed to adopt or enforce regulations to protect patients against hacking attempts. To date there have been no reports of such hacking—but then again, it would be extremely difficult to detect this type of foul play. The threat is sufficiently viable that former Vice President Dick Cheney's doctor ordered the disabling of his heart implant's wireless capability, apparently to prevent a hacking attempt, while Cheney was in office.[110]

As will be discussed below, the FTC has taken the lead in data security regulatory efforts in the U.S. The FTC and the Food and Drug

---

[107] *Id.*
[108] *See, e.g.,* Gregory Mandel, *Nanotechnology Governance*, 59 ALA. L. REV. 1324 (2008)
[109] *See, e.g.,* H@cking Implantable Medical Devices, INFOSEC INSTITUTE (Apr. 28, 2014), http://resources.infosecinstitute.com/hcking-implantable-medical-devices/.
[110] Benjamin Wittes & Jane Chong, *Our Cyborg Future: Law and Policy Implications* BROOKINGS (September 2014), http://www.brookings.edu/research/reports2/2014/09/cyborg-future-law-policy-implications.

Administration (FDA), will likely take the lead in regulating data security and cybersecurity for implantable devices.[111]

The FTC has mandated notice be given by devices capable of physically harming consumers.[112] For example, in *In re Consumer Direct*, the FTC charged that a producer of "exercise" equipment called the "Amazing Gut Buster" failed to adequately warn consumers that "when performed as directed the Gut Buster exercises pose a risk of injury to users from snapping or breakage of the product's spring or other parts."[113] This failure to warn consumers was alleged to be an unfair trade practice by the FTC.[114]

---

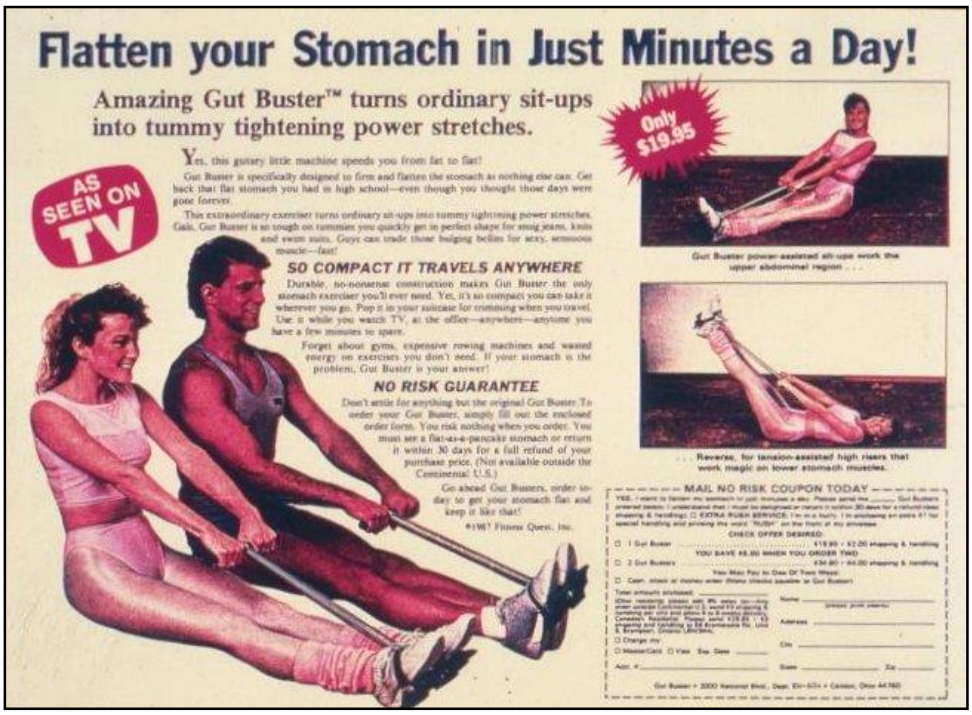
[111] *See* Cybersecurity, FDA, http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/ucm373213.htm (last visited Nov. 21, 2014); Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software, FDA (Jan. 14, 2005), *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf; Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, FDA (Oct. 2, 2014), *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf.

[112] *See, e.g.,* In re Consumer Direct Inc. et. al., 118 F.T.C. 923 (1990), https://www.ftc.gov/sites/default/files/documents/commission_decision_volumes/volume-113/volume113_923-1015.pdf.

[113] *Id.*

[114] *Id.*

Figure 3. The Wonderfully Dated Ad for the "Amazing Gut-Buster."



Thus, the FTC has the power to mandate notice and reasonable data security for implantable robotic-like devices. As will be discussed below, these are just two of the tools that enable the FTC to regulate the growing field of consumer robotics.

***

The issues described above are just a small sample of the potential complications that will arise as consumers embrace robots. In the next part, I will describe how the FTC has the ability to competently regulate consumer robotics.

II. THE FTC HAS THE ABILITY TO ADDRESS CONSUMER ROBOTICS

There seem to be three crucial concepts for safe manufacture and use of consumer robots: communications, design, and organizational procedure. Companies must accurately communicate to consumers the efficacy of robots as well as any costs and risks of use. Companies should also use reasonable care when designing robots and avoid culpably providing the

means and instrumentalities for wrongful or harmful conduct. Finally companies that make robots should implement organizational procedures such as administrative safeguards and training to keep robots and the data they collect secure and private. The FTC has proven to be a competent regulator in these areas.

The FTC's existing framework for protecting consumers from fraud, data breaches, privacy harms, and exploitation is robust enough to adequately protect consumers and clear enough to notify commercial entities of their obligations when designing, selling, and using robots that interact with consumers. Notably, the FTC is enabled by broad regulatory authority and a diverse set of tools to respond to problems.

1. *Broad Regulatory Authority*

The FTC has a very interesting history.[115] Originally created to combat harmful monopolies, the Wheeler-Lea Amendments to Section 5 of the FTC Act to prevent "Unfair or deceptive trade practices" in addition to "unfair methods of competition."[116] This is a very broad charge for Congress to delegate to an administrative agency. Any material representation, omission or practice that is likely to mislead a reasonable consumer is actionable.[117] Similarly, the FTC's unfairness authority is also far-reaching.

According to the FTC, "The present understanding of the unfairness standard is the result of an evolutionary process. The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that

---

[115] *See, e.g.,* Our History, FTC, https://www.ftc.gov/about-ftc/our-history, (last accessed Mar. 19, 2015); *see also* CHRIS HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (forthcoming 2016), https://hoofnagle.berkeley.edu/ftcprivacy/; Gerald C. Henderson, THE FEDERAL TRADE COMMISSION: A STUDY IN ADMINISTRATIVE LAW AND PROCEDURE (1924); Huston Thompson, *Highlights in the Evolution of the Federal Trade Commission*, 8 GEO. WASH. L. REV. 257 (1939); Eugene R. Baker and Daniel J. Baum, *Section 5 of the Federal Trade Commission Act: A Continuing Process of Redefinition*, 7 VILL. L. REV. 517 (1962).

[116] Federal Trade Commission Act, Pub. L. No. 75-447, § 3, 52 Stat. 111 (1938).

[117] *See* FTC Statement on Deception, Appended to Cliffdale Associates, Inc., 103 F.T.C. 110, 174 (1984).

would not quickly become outdated or leave loopholes for easy evasion."[118] Notably, the FTC can find a practice unfair even when it is otherwise legally permissible.[119]

Regarding the meaning of unfairness, the House Conference Report regarding unfairness stated: "It is impossible to frame definitions to embrace all unfair practices. There is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again. If Congress were to adopt the method of definition, it would undertake an endless task."[120] In short, it is the FTC (subject to judicial review) that has been tasked with identifying unfair trade practices.

In its statement on unfairness, the FTC cited the Supreme Court's explicit recognition that unfairness should evolve over time instead of an ex ante prescription.[121] The Court stated that the term unfairness "belongs to that class of phrases which do not admit of precise definition, but the meaning and application of which must be arrived at by what this court elsewhere has called 'the gradual process of judicial inclusion and exclusion."[122]

This broad scope is ideal for a regulatory agency in charge of responding to challenges posed by new technologies. Chris Hoofnagle observed, "[With Section 5], Congress chose a broad, vaguely-defined mandate to address consumer protection. The value of this vagueness comes in the FTC's flexibility to address new problems."[123] For example, Hoofnagle noted that "for the first thirty years of the FTC, the agency was focused on

---

[118] FTC Policy Statement on Unfairness, Appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984). See 15 U.S.C. § 45(n).
[119] Spiegel v. FTC, 540 F.2d 287, 292 (1976) (citing FTC v. Sperry & Hutchison, Co., 405 U.S. 233 (1972)) ("[T]he Supreme Court left no doubt that the FTC had the authority to prohibit conduct that, although legally proper, was unfair to the public.").
[120] FTC v. Sperry and Hutchinson, supra at 240 (quoting from House Conference Report No. 1142, 63 Cong., 2d Sess., 19 (1914)).
[121] *Id.* (citing FTC v. Raladam Co., 283 U.S. 643, 648 (1931). See also FTC v. R.F. Keppel & Bro., 291 U.S. 304, 310 (1934) ("Neither the language nor the history of the Act suggests that Congress intended to confine the forbidden methods to fixed and unyielding categories")).
[122] *Id.*
[123] *Id.* at 30; CHRIS HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (forthcoming 2016), https://hoofnagle.berkeley.edu/ftcprivacy/.

print advertising. With the rise of radio advertising, the agency was able to pivot and investigate false claims on the airwaves, without having to have Congress enact a law."[124] The same was true for television, as the FTC again recalibrated how technology can be used to deceive or harm consumers.[125] The same will be true for robots. As the FTC's foray into the "Internet of Things" makes clear, the FTC does not need a new authorization of power to tackle a new technology. It is sufficient if a company uses a new technology in commerce to harm or mislead consumers.

Additionally, the FTC can regulate consumer harms that fall outside the scope of traditional torts and other regulatory efforts. Although the linchpin of unfairness is harm, the FTC has not limited the kinds of harm that necessary to establish a practice as unfair. The harm simply must be substantial.[126]

The most dominant kind of substantial harm asserted by the FTC has been monetary.[127] Relevant to our hypothetical robot's underhanded upsell, the FTC listed as an example of monetary harm in its statement on unfairness "as when sellers coerce consumers into purchasing unwanted goods." The FTC has also stated that "[U]nwarranted health and safety risks may also support a finding of unfairness," citing a case where a company distributed free-sample razor blades in a way easily obtainable by small children.[128] Thus, certain nudgebots, algorithms, products for cyborgs, and other poorly designed robots may also be unfair due to health and safety risks.

However, many manipulative tactics by robots might fall outside of this jurisdiction. For years the accepted wisdom was that "Emotional impact and other more subjective types of harm, on the other hand, will not

---

[124] *Id.*
[125] *Id.*
[126] FTC Policy Statement on Unfairness, Appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984). See 15 U.S.C. § 45(n) ("First of all, the injury must be substantial. The Commission is not concerned with trivial or merely speculative harms.").
[127] *Id.*
[128] *Id.* (citing Philip Morris, Inc., 82 F.T.C. 16 (1973)) and noting that "Of course, if matters involving health and safety are within the primary jurisdiction of some other agency, Commission action might not be appropriate.").

ordinarily make a practice unfair."[129] However, notions of unfairness harm have been steadily evolving over the past twenty years.[130] In a remarkable footnote in the *Wyndham* opinion challenging the FTC's authority to regulate data security, Judge Salas noted the dispute over whether non-monetary injuries are cognizable under Section 5. She seemed open to recognizing non-monetary harm, stating, "…the court is not convinced that non-monetary harm is, as a matter of law, unsustainable under Section 5 of the FTC Act…."[131]

If non-monetary harm were to be recognized, it is possible that the FTC could include emotional harms related to our dependence on and emotional vulnerability to robots and possibly even transference issues, particularly with respect to small children. Even if these harms are incremental for one individual, if they are collectively a problem they might still be actionable. The FTC has clarified that "An injury may be sufficiently substantial, however, if it does a small harm to a large number of people…."[132]

The FTC's broad authority would be particularly useful given that these are still early days for consumer robotics. In supporting his claim that robots warrant exceptional legal treatment, Ryan Calo observed, "Robots display increasingly emergent behavior, permitting the technology to accomplish both useful and unfortunate tasks in unexpected ways."[133] It is difficult to predict the many different issues that might arise when robots are adopted by consumers. While many existing laws might cover emergent issues, other problems might fall through the cracks. The

---

[129] *Id.* ("Thus, for example, the Commission will not seek to ban an advertisement merely because it offends the tastes or social beliefs of some viewers, as has been suggested in some of the comments.").
[130] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).
[131] FTC v. Wyndham Worldwide Corp., No. 13-1887 Slip Op. (April 7, 2014 D.N.J.) at 28, footnote 15. Ultimately, Judge Salas concluded that "the Court need not reach this issue given the substantial analysis of the substantial harm element above." *Id.*
[132] FTC Policy Statement on Unfairness, Appended to International Harvester Co., 104 F.T.C. 949, 1070 at fn12 (1984). See 15 U.S.C. § 45(n).
[133] Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. (forthcoming 2015).

breadth of Section 5 allows it to serve as a safety net to nimbly respond to unanticipated problems.

There are limits to the FTC's authority. The agency does not have authority over non-profit organizations and common carriers. It cannot regulate consumers who harm other consumers in a non-commercial context. As mentioned, its authority to regulate data security is being challenged in court.[134] Notwithstanding these limitations, the FTC has enough authority to competently address most cognizable consumer harms from robots.

2. *Diverse and Effective Toolkit*

In addition to having a general grant of authority broad enough to regulate consumer robotics, the FTC has developed several specific bodies of jurisprudence that it can rely upon to address established and novel harms related to consumer robotics. The FTC has a developed record of regulating when and how a company must disclose information to avoid deception and protect a consumer from harm. The FTC has also recently developed secondary liability and means and instrumentality theories for unfair and deceptive technological design and organizational policies.

a. Disclosures

One of the most effective tools the FTC has is the power to regulate company disclosures in advertisements and other statements made in commerce. Because robots are relatively new, consumer expectations are not established. There are many things a robot might be capable or incapable of that must be disclosed to consumers to avoid deception. The FTC's disclosure jurisprudence is thus an ideal starting point for its entry into consumer robotics.

The FTC's mandated notice jurisprudence is robust and established. Generally speaking a disclosures are required whenever they are

---

[134] Woodrow Hartzog & Daniel Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. (forthcoming 2015); FTC v. Wyndham Worldwide Corp., No. 13-1887 Slip Op. (April 7, 2014 D.N.J.); Order Denying Respondent LabMD's Motion to Dismiss, In the Matter of LabMD, No. 9357, http://www.ftc.gov/sites/default/files/documents/cases/140117labmdorder.pdf.

necessary to prevent a communication or trade practice from being deceptive.[135] Disclosures must be clear and conspicuous.[136] The agency has detailed specific rules regarding what constitutes effective notice.[137] For traditional advertising, the four major factors that constitute adequate notice for the FTC are:

- Prominence: Is the disclosure big enough for consumers to notice and read?
- Presentation: Is the wording and format easy for the consumers to understand?
- Placement: Is the disclosure where consumers will look?
- Proximity: Is the disclosure close the claim it qualifies?[138]

The FTC also looks to repetition, the use of multiple media for communications, and whether there were distracting factors that might diminish the effectiveness of a disclosure, particularly online.[139]

The FTC has also developed nuanced theories regarding deception by omission, use of scientific data and endorsements.[140] The FTC is also not

---

[135] FTC, .com Disclosures: How to Make Effective Disclosures in Digital Advertsing, FTC (March 2013), https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf.
[136] *See,e .g.,* 16 CFR § 14.9 ("clear and conspicuous" disclosure must be made in the language of the target audience); Donaldson v. Read Magazine, Inc., 333 U.S. 178 (1948); FTC, .com Disclosures: How to Make Effective Disclosures in Digital Advertsing, FTC (March 2013), https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf.
[137] FTC, .com Disclosures: How to Make Effective Disclosures in Digital Advertsing, FTC (March 2013), https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf.
[138] *Id.*; *see also* Donaldson v. Read Magazine, Inc., 333 U.S. 178 (1948); BUY.COM, Inc., C-3978 (Sept. 8, 2000) (consent order); Hewlett-Packard Co., File No. 002-3220, and Microsoft Corp., File No. 002-3331 (proposed consent agreements published for public comment April 4, 2001); Häagen-Dazs Co., 119 F.T.C. 762 (1995) (consent order).
[139] *Id.*; 16 C.F.R. § 239.2(a) (mandating disclosure "simultaneously with or immediately following the warranty claim" in the audio portion or "on the screen for at least five seconds" in the video portion).
[140] *See* REBECCA TUSHNET & ERIC GOLDMAN, ADVERTISING & MARKETING LAW: CASES AND MATERIALS (2nd ed. 2014).

bound by the fine print, which will keep harmful terms that nobody reads from being enforceable.[141]

Disclosures regarding robots present both substantive and procedural disclosure issues. First, given that people have a tendency to treat robots as social agents, must additional disclosures be made beyond typical contexts involving physical safety, endorsements, and product efficacy? Recall Anthro-Rocco, the friendly vacuum cleaner. If indeed Rocco is programmed to upsell me by preying on my emotional bond with it, must the maker actively disclose the fact that Rocco is designed to form emotional attachment? Should the makers of Boxie disclose the fact that the robot's cuteness is a tool for information extraction?

If so, why? Are people's relationships and our resulting vulnerability with robots sufficiently unique to justify this sort of exceptionalism? If not, does this mean that there is no limit to the extent to which companies can leverage human emotions and agency towards robots behind the curtains?

The second disclosure issue presented by robots concerns how notice is given. Given that robots *themselves* are capable of marketing and making the FTC's required disclosures and that people's communication with robots can be reciprocal, should the rules regarding the four P's of disclosure (prominence, presentation, placement, proximity) reflect the fact that the robot will often be in the best position to make a "just in time" disclosure?

When the consumer good is also the advertising medium, it is not always clear when routine communication also constitutes an advertisement. Since a robot can be programmed to sense context and make disclosures during its use and not just at the purchase point, it is possible the FTC will have different rules for such experiential, automated products. In fact, the

---

[141] *See, e.g.,* See BUY.COM, Inc., C-3978 (Sept. 8, 2000) (consent order); Hewlett-Packard Co., File No. 002-3220, and Microsoft Corp., File No. 002-3331 (proposed consent agreements published for public comment April 4, 2001); REBECCA TUSHNET & ERIC GOLDMAN, ADVERTISING & MARKETING LAW: CASES AND MATERIALS (2nd ed. 2014) ("Small print, by itself or combined with other features such as color, contrast and placement, is almost always deemed ineffective because consumers are unlikely to wade through a long paragraph of fine print in order to find significant information.").

FTC might eventually issue new guidance for robot disclosures as it did with disclosures on the Internet.[142]

New disclosure rules for robots would be an ideal opportunity to rethink modern notice requirements. Existing notice and choice regimes have been asked to do more than they are capable of. But new technologies open up the opportunity for innovative new forms of notice. Ryan Calo has proposed a policy shift towards "visceral notice," that is, "[leveraging] a consumer's very experience of a product or service to warn or inform."[143] Might robots provide new opportunities for such kinds of notice? In addition to warning consumers through their speech, robots can warn consumers through design signals like a bright red light as well as physical action such as waving hands or holding up a palm to signal "stop."

The FTC's mandated disclosure framework is general enough to be applied to consumer robots. And the FTC has the ability to refine and articulate technology-specific disclosure rules if necessary. This makes its disclosure jurisprudence the best place to begin addressing consumer robotics.

b. Design and Secondary Liability

One of the FTC's most promising recent approaches to data protection is its embrace of design-based solutions, defined broadly as attempts to create or modify a technology, architecture, or organizational structure or procedure *ex ante* as an attempt to reduce the likelihood of a harm.

Design-based solutions are prospective and implicitly embrace a probabilistic notion of protection. That is, in most circumstances, they make consumer harms more unlikely, but not impossible. Design-based solutions are also indirect in that they affect environments and procedures rather than directly prohibiting certain kinds of conduct. Often, the goal of design is to raise the transactional costs of a harmful

---

[142] FTC, .com Disclosures: How to Make Effective Disclosures in Digital Advertsing, FTC (March 2013), https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf.
[143] M. Ryan Calo, *Against Notice Skepticism in Privacy (And Elsewhere)*, 87 NOTRE DAME L. REV. 1027 (2012).

activity so high that most potential third party bad actors simply won't succeed or even bother. Other times design is used to reduce the odds that consumers will harm themselves.

Data security is itself one of the most established design-based protection strategies. By anonymizing information and creating protocols to keep information hard for hackers to find, access, or use, all but the most determined attackers usually do not attempt or succeed in accessing well-protected data. As any data security professional will likely testify to, no data security is perfect, but it can be good enough to have confidence that certain data sets will probably remain secure against all but the most sophisticated and motivated attackers.

Design-based protections such as handrails on stairs and fencing on balconies keep us from slipping and falling. So too can software design encourage or discourage irresponsible information sharing. Ultimately, everyone is limited and guided by the affordances of their environment.

The FTC has begun to embrace design as a regulatory focus. Many privacy related unfairness complaints by the FTC are attempts to discourage certain types of design. For example, the FTC has found the design of websites and software to be unfair. In *Sony BMG*, digital rights management (DRM) software was installed on consumers' computers in such a way that consumers were unable to find or remove the software through reasonable effort.[144] If consumers attempted to remove the software, it would render their CD-ROM drive inoperable. The FTC deemed the software design to be unfair.[145] The FTC recently brought a complaint against the maker of a flashlight mobile app alleging that "the company deceived consumers by presenting them with an option to not

---

[144] The term DRM is generally used to technological measures that allow digital content owners to control how their content is used. *See* Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575 (2003) ("In an effort to control the proliferation of unauthorized copies, and to maximize profit from information goods distributed over the Internet, copyright owners and their technology partners are designing digital rights management ("DRM") technologies that will allow more perfect control over access to and use of digital files.")

[145] In re Sony BMG Music Entm't, FTC File No. 062 3019, No. C-4195, at 6 (June 2007), available at http://www.ftc.gov/sites/default/files/documents/cases/2007/06/0623019d0070629.pdf .

share their information, even though it was shared automatically rendering the option meaningless."[146]

Related to design are the default settings for data sharing, as these shape consumer behavior. In *Frostwire*, the FTC alleged that failure to notify users that many pre-existing files on consumer computers would be designated for public sharing constituted an unfair design.[147] Users who did not wish to share a large number of files had to go through the burdensome process of protecting the files one at a time by unchecking many pre-checked boxes designating the files for sharing. The FTC noted that deceitful or obstructionist default settings constitute an unfair design feature.[148]

Since the FTC has more flexibility regarding harm than tort law, the FTC is more capable of addressing small and nuanced changes in design that affect consumers. For example, if a robot's settings or design was deceptive or unfair because of a checked default, the FTC could pressure companies to make a change that might not even be relevant three years from now given the pace of change in consumer robotics.[149]

The FTC has also embraced design, such as the features of a user interface, when considering whether disclosures are adequate. In *Path*, the FTC asserted that the customizable settings and interactive features of a mobile app were deceptive.[150] In a non-privacy related complaint, the FTC alleged that the design of the Apple's mobile operating system's user

---

[146] Android Flashlight App Developer Settles FTC Charges It Deceived Consumers, FTC (Dec. 5, 2013), http://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived.

[147] Complaint for Permanent Injunction and Other Equitable Relief at 13, FTC v. Frostwire, LLC, No. 11-cv-23643 (S.D. Fla. Oct. 12, 2011), available at http://www.ftc.gov/os/caselist/1123041/111011frostwirecmpt.

[148] *Id.* at 15--16, 19.

[149] United States v. Path, Inc., No. 13-cv-00448 (N.D. Cal. Feb. 8, 2013) (consent decree & order), available at http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf

[150] United States v. Path, Inc., No. 13-cv-00448, at 8 (N.D. Cal. Feb. 8, 2013) (consent decree & order), available at http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf.

interface resulted in unfair billing of in-app charges.[151] The FTC's theory of design regulation would also logically apply to robots.

The FTC has also developed a theory of culpability for design choices that indirectly harm consumers. Its secondary liability approach resembles theories of contributory infringement and vicarious liability.[152] Facilitating the wrongful conduct of another also triggers FTC condemnation. For example, in *DesignerWare*, the FTC alleged that "[b]y furnishing others with the means to engage in the unfair practices . . . respondents have provided the means and instrumentalities for the commission of unfair acts and practices and thus have caused or are likely to cause substantial injury to consumers that cannot be reasonably avoided and is not outweighed by countervailing benefits to consumers or competition."[153]

In *FTC v. Neovi*, also known as the "Qchex" dispute, the FTC asserted a theory of indirect liability against a company that created a check creation and delivery website but failed, by design, to verify that customers were rightfully drawing upon accounts they identified.[154] The FTC has also stated that providing the means and instrumentalities to install spyware

---

[151] In the Matter of Apple, Inc., Complaint, http://www.ftc.gov/sites/default/files/documents/cases/140115applecmpt.pdf.

[152] Jay Dratler, Jr., *Common-Sense (Federal) Common Law Adrift in A Statutory Sea, or Why Grokster Was A Unanimous Decision*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 413, 434 (2006) ("[S]econdary liability in copyright is federal common law...."); Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, LTD., 545 U.S. 913 (2005) ("Although "[t]he Copyright Act does not expressly render anyone liable for infringement committed by another," these doctrines of secondary liability emerged from common law principles and are well established in the law.") (citing Sony Corp. v. Universal City Studios, 464 U.S., at 434, 486 (Blackmun, J., dissenting); Kalem Co. v. Harper Brothers, 222 U.S. 55, 62—63 (1911); Gershwin Pub. Corp. v. Columbia Artists Management, supra, at 1162; 3 M. Nimmer & D. Nimmer, Copyright, §12.04[A] (2005)); A & M Records, Inc. v. Napster, Inc. 239 F.3d 1004 (9th Cir. 2001).

[153] In re DesignerWare, LLC, FTC File No. 112 3151, No. C-4390 (F.T.C. Apr. 11, 2013), available at http://www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwarecmpt.pdf.

[154] FTC v. Neovi, Inc., Complaint, 06CV-1952-WQH-JMA, https://www.ftc.gov/sites/default/files/documents/cases/2006/10/060919neovicmplt.pdf (S.D. Cal. 2006).

and access customer's personal information was an unfair trade practice.[155]

The FTC has only occasionally pursued a claim of indirect liability against companies. It is unlikely to pursue an action against a robotics company under this theory save for extreme circumstances. Yet it is worth noting that much of the discussion surrounding ethics and robotics has to do with design choices.[156] Should home care robots be designed to record private moments like going to the bathroom? Should robots be programmable or controllable by anyone, or just owners? What kind of authentication and verification protocols should robots have? Should robots be designed to be "closed," in the sense that they have a set, dedicated function and run only proprietary software?[157] Or can companies design robots to be "open" without incurring liability, in the sense that they have a nondedicated use, nondiscriminatory software, and modular design?[158]

Questions like these reflect that fact that rules for the design of robots can be just as consequential as rules for their ultimate use. The FTC is one of the few agencies capable of addressing design issues.

c. Organizational Procedures and Data Protection

Data security is one of the most crucial components for consumer robotics. If consumers cannot trust robots and companies that make robots with their personal information, the consumer robotics industry will never get off the ground. Data security is a process companies must

---

[155] In re CyberSpy Software, LLC and Trace R. Spence, FTC File No. 082 3160, No. 08-CV-01872 (F.T.C. Nov. 17, 2008)

[156] *See generally* ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS 187, 194 (Patrick Lin, Keith Abney & George A. Bekey ed. 2012); Laurel Riek, Woodrow Hartzog, Don Howard, AJung Moon, & Ryan Calo, The Emerging Policy and Ethics of Human Robot Interaction. In Proceedings of the 10th ACM/IEEE Conference on Human-Robot Interaction (HRI) (2015); M. Ryan Calo, *Open Robotics*, 70 MD. L. REV. 101 (2011); Aimiee Van Wynsberghe, *A Method for Integrating Ethics Into the Design of Robots*, 40 INDUSTRIAL ROBOT: AN INTERNATIONAL JOURNAL 433 (2013); Aimiee Van Wynsberghe, Designing Robots for Care: Care Centered Value-Sensitive Design, 19 SCIENCE AND ENGINEERING ETHICS 407 (2013).

[157] *See* M. Ryan Calo, *Open Robotics*, 70 MD. L. REV. 101 (2011).

[158] *Id.*

engage in involving identification of assets and risk, data minimization, implementation of administrative, technical, and physical safeguards, and the development of a data breach response plan.[159] But, at base, it is a component necessary to build consumer trust.

The FTC has established a robust data security jurisprudence, filing over 50 data security complaints in the past fifteen years that obligate companies collecting and storing personal information to provide reasonable data security requirements.[160] These obligations are not limited to Internet companies, as demonstrated by complaints against traditional retailers and more relevantly makers of devices for the "Internet of Things."[161]

In many ways, the FTC's *TRENDnet* case, which was the agency's first "Internet of Things" complaint, can be seen as a bridge between its Internet-related complaints that have dominated its jurisprudence over the past fifteen years and the eventual attention that must be given to consumer robotics. At one level, this case simply involves deceptive promises of security and unreasonable data security design for Internet-connected baby monitors. These monitors were compromised to the shock and dismay of sleeping toddlers and adults in the U.S.[162] Yet the complaint also signaled that new technologies must protect consumers in the same way existing established technologies do.

Privacy rules can also be conceptualized as a process. The FTC has recently embraced the concept of "privacy by design," broadly described by the agency as a baseline principle encouraging companies to "promote consumer privacy throughout their organizations and at every stage of the development of their products and services."[163] According to the FTC,

---

[159] FEDERAL TRADE COMMISSION, *Commission Statement Marking the FTC's 50th Data Security Settlement* (January 31, 2014) http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.
[160] In re TRENDnet, Complaint, https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.
[161] *See, e.g.,* In re BJ's Wholesale Club, Inc., 140 F.T.C. 465, 468 (2005) (complaint); In re TRENDnet, Complaint, https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.
[162] *Id.*
[163] FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 2 (2012), available at http://

"The concept of privacy by design includes limitations on data collection and retention, as well as reasonable security and data accuracy. By considering and addressing privacy at every stage of product and service development, companies can shift the burden away from consumers who would otherwise have to seek out privacy protective practices and technologies."[164]

The FTC has even required companies to implement privacy by design in its consent orders through a "comprehensive privacy program."[165] These programs require, among other things, the designation of an employee in charge of the program, risk assessments, design and implementation of privacy controls, diligence in working with third party contractors, and regular re-evaluation and adjustment of the program.[166] Processes like these could also work for companies that design robots, particularly those that collect personal information.

***

In this part I have made the argument that the FTC *can* regulate consumer robotics and has some unique tools and theories to do so effectively. In the next part, I will argue that the FTC *should* embrace consumer robotic so that the robotics industry can continue to flourish while consumers are protected.

III. THE FTC SHOULD TAKE THE LEAD ON REGULATING CONSUMER ROBOTICS

Numerous federal, state, and non-governmental bodies will inevitably have some role in regulating consumer robotics. For example, the Consumer Product Safety Commission (CPSC), charged with "protecting the public from unreasonable risks of injury or death associated with the

---

www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[164] *Id.*

[165] In re Snapchat, Consent Order, https://www.ftc.gov/system/files/documents/cases/140508snapchatorder.pdf.

[166] *Id.*

use of the thousands of types of consumer products," is likely to get involved if robots start physically harming consumers.[167]

The Federal Aviation Administration has already begun the process of regulating drones, which are already commercially available.[168] The Food and Drug Administration (FDA) regulates implantable devices and telepresence surgical robots.[169] The National Highway Traffic and Safety Administration (NHTSA) has released a preliminary report outlining a plan to ensure that automated, self-driving cars are safe.[170] The International Organization for Standardization has released numerous standards for safety requirements for industrial and personal care

---

[167] Consumer Products Safety Commission, About, http://www.cpsc.gov/en/About-CPSC/ (last accessed Mar. 19, 20150.

[168] FAA, Overview of Small UAS Notice of Proposed Rulemaking, Feb. 15, 2015, http://www.faa.gov/regulations_policies/rulemaking/media/021515_sUAS_Summary.pdf.

[169] *See* Cybersecurity, FDA, http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/ucm373213.htm (last visited Nov. 21, 2014); Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software, FDA (Jan. 14, 2005), *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf; Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, FDA (Oct. 2, 2014), *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

[170] U.S. Department of Transportation Releases Policy on Automated Vehicle Development, NHTSA, May 30, 2013, http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+Department+of+Transportation+Releases+Policy+on+Automated+Vehicle+Development.

robots.[171] This is to say nothing of the effect that contracts, insurance, and products liability laws are likely to have on consumer robotics.[172]

It is even possible that regulatory bodies will be formed to address robots. Ryan Calo has proposed a new Federal Robotics Commission, which would, at least initially, play an advisory role for other regulatory bodies and companies.[173] Calo recognized that an agency could help responsibly integrate robotics technologies into American society.[174] According to Calo, "Robots, like radio or trains, make possible new human experiences and create distinct but related challenges that would benefit from being

---

[171] ISO 13482:2014, Robots and robotic devices -- Safety requirements for personal care robots, http://www.iso.org/iso/catalogue_detail.htm?csnumber=53820; ISO 10218-1:2011, Robots and robotic devices -- Safety requirements for industrial robots -- Part 1: Robots, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51330; ISO 10218-2:2011, Robots and robotic devices -- Safety requirements for industrial robots -- Part 2: Robot systems and integration, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=41571; ISO/DTS 15066, Robots and robotic devices -- Safety requirements for industrial robots -- Collaborative operation, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62996,

[172] *See, e.g.,* David C. Vladeck, *Machines Without Principals: Liability Rules and Artificial Intelligence*, 89 WASH. L. REV. 117, 121 (2014); Patrick Hubbard, Regulation and Liability for Risks of Physical Injury from "Sophisticated Robots," In Proceedings of We Robot Conference, University of Miami, 2012, http://robots.law.miami.edu/wp-content/uploads/2012/01/Hubbard_Sophisticated-Robots-Draft-1.pdf; Bryant Walker Smith, Proximity-Driven Liability, 102 Geo. L.J. (forthcoming 2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2336234; Diana Marina Cooper, A Licensing Approach to Regulation of Open Robotics, In Proceedings of We Robot Conference, Stanford University, 2013, http://conferences.law.stanford.edu/werobot/wp-content/uploads/sites/29/2013/04/Cooper_Diana.pdf.

[173] Ryan Calo, *The Case for a Federal Robotics Commission*, BROOKINGS (September 2014), http://www.brookings.edu/research/reports2/2014/09/case-for-federal-robotics-commission ("The institution I have in mind would not "regulate" robotics in the sense of fashioning rules regarding their use, at least not in any initial incarnation. Rather, the agency would advise on issues at all levels—state and federal, domestic and foreign, civil and criminal—that touch upon the unique aspects of robotics and artificial intelligence and the novel human experiences these technologies generate.").

[174] *Id.* ("The alternative, I fear, is that we will continue to address robotics policy questions piecemeal, perhaps indefinitely, with increasingly poor outcomes and slow accrual of knowledge.").

examined and treated together. They do require special expertise to understand and may require investment and coordination to thrive."[175]

As of yet, however, no existing body has taken the lead to guide the development of consumer robotics to protect consumers. Federal agency leadership would be useful to help develop consistent standards, encourage cooperation among regulatory bodies, and shield off burdensome, knee-jerk, and over-reactive regulatory efforts by Congress or other lawmaking bodies. In this part, I argue that the FTC should take this leadership role in consumer robotics.

The FTC is best positioned to take the lead on consumer robotics issues because it has developed a robust body of law to draw from and has a track-record of fostering nascent technologies like the Internet. This will allow the agency to enable consumer robotics to flourish while protecting consumers in a way consistent with established consumer protection goals and law. The FTC gives deference to industry standards where relevant, which will keep the law of consumer robotics from being arbitrary and disconnected from practice.

The agency is capable of responding to technological change quickly but with stability, which is a necessity in the rapidly-evolving field of robotics. The FTC regularly cooperates with other regulatory bodies and can use this experience to build consensus and consistency. Finally, the FTC can use Section 5 as a safety net to address emergent issues in consumer robotics that are currently unforeseeable or have not yet been realized.

1. *Established Body of Law and Authority*

When a federal agency operates for 100 years, it is bound to establish a robust body of law. FTC official actions and legal resources can take the form of advisory opinions, advocacy filings, cases, closing letters, volumes of commission decisions, notices in the Federal Register, press releases, public comment initiatives, public events, public statements, reports, and

[175] *Id.*

rules.[176] However, the two most prominent forms of FTC jurisprudence come from rules and cases, namely complaints.

The FTC has filed thousands of complaints regarding advertising and marketing, credit and finance, and privacy and security in various industries such as alcohol, appliances, automobiles, clothing, finance, franchises, business opportunities, and investments, funerals, human resources, jewelry, real estate and tobacco.[177]

These cases establish and develop the FTC's body of law in incremental steps. In research regarding the FTC's regulation of privacy, Daniel Solove and I have argued that the FTC's complaints functionally operate as a body of common law, even though they are not judicial opinions with precedential value.[178] The FTC remains consistent with these complaints and practitioners view them has having precedential weight.[179]

Moreover, minus a few exceptions involving unfairness such as data security, the FTC's regulation of marketing, finance, and privacy is well-established.[180] It would be relatively uncontroversial to apply the FTC's framework for disclosure, substantiation, endorsements, or trade puffery to robots in applicable scenarios. Robots are not so different from other technologies and trade practices that the FTC's theories of design, indirect liability, and data protection would be inapplicable. Thus the FTC is preferable as a leader in this field because it can leverage the great weight of its jurisprudence to protect consumers against the non-exceptional problems presented by consumer robotics.

---

[176] Legal Resources, FTC, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=249 (last accessed Mar. 19, 2015).

[177] Legal Resources, Cases, FTC, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=249 (last accessed Mar. 19, 2015).

[178] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 619 (2014) ("Although the FTC's privacy cases nearly all consist of complaints and settlements, they are in many respects the functional equivalent of common law. While the analogy to traditional common law has its limits, it is nonetheless a useful frame to understand the FTC's privacy jurisprudence.").

[179] *Id.*

[180] Woodrow Hartzog & Daniel Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. (forthcoming 2015).

2. *Accommodation of Nascent Technologies*

In the past, the FTC has approached promising technologies with a light regulatory touch when they were new and only increased regulatory efforts once those technologies became more established. The best example of this is the Internet. The incredible potential of the Internet first became clear to both regulators and the public in the 1990s. Regulators generally did not want to stifle this technology, which could change the world for the better, with burdensome laws. This included the FTC, which first embraced a self-regulatory regime for online privacy and then eventually shifted over into a co-regulatory regime.[181]

A similar approach seems wise for consumer robotics as well. As discussed above, the non-exceptional aspects of consumer robotics, that is, those with existing analogs, are safely regulated under established FTC jurisprudence. Robotics companies should not be allowed to deceive or harm consumers simply because they are new.

However, the exceptional aspects of consumer robotics should receive a reasonably light regulatory touch for now. This means a preference for disclosure requirements over conduct prohibitions and a case-by-case approach instead of rigorous rulemaking. Before launching into too many enforcement actions, the FTC should continue its tradition of investigation and guidance by holding public events on consumer robotics and issuing reports and white papers to guide norms in relevant areas.

---

[181] *See* FTC, Self-Regulation and Privacy Online: A Report to Congress 12-14 (1999) ("[T]he Commission believes that legislation to address online privacy is not appropriate at this time."); Robert Pitofsky, Chairman, FTC, Prepared Statement of the Federal Trade Commission on "Consumer Privacy on the World Wide Web" (July 21, 1998), available at http:// www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-consumer-privacy-world-wide-web/privac98.pdf ("[T]he Commission's goal has been ... to encourage and facilitate self-regulation as the preferred approach to protecting consumer privacy online."); Robert Pitofsky, Chairman, FTC, Prepared Statement of the Federal Trade Commission on "Self-Regulation and Privacy Online" (July 13, 1999), available at http://www.ftc.gov/public-statements/1999/07/prepared-statement-federal-trade-commission-self-regulation-and-privacy (describing self-regulation as "least intrusive and most efficient means to ensure fair information practices online").

The FTC also has limited resources, which means that it places great emphasis on prioritization. In the privacy context, the FTC files only about 10-15 complaints per year.[182] The likelihood of being the subject of an FTC complaint is quite small. The result is that the FTC generally stays away from the grey areas and largely pursues only the most egregious cases of wrongdoing.[183]

Thus, the FTC's constraints help ensure that the consumer robotics industry has the room it needs to grow. Most actions by robotics companies will not result in an agency complaint and only the most serious misrepresentations and unfair actions will trigger enforcement. This preservation of grey area for robotics companies will allow the industry to flourish while consumers calibrate appropriate expectations surrounding the use and efficacy of robots.

3. *Deference to Industry*

The FTC also has a track record of deferring to industry practices to establish co-regulatory regimes. The most prominent recent example of this deference is with the FTC's regulation of data security. The FTC generally requires "reasonable" data security from companies that collect consumer information.[184] In a statement issued in conjunction with the FTC's 50th data security complaint, the FTC stated, "The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities."[185]

The FTC has implicitly and explicitly represented that it looks to industry standards to guide its enforcement, particularly when determining what

---

[182] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 619 (2014).
[183] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 619 (2014); Woodrow Hartzog & Daniel Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. (forthcoming 2015).
[184] FEDERAL TRADE COMMISSION, *Commission Statement Marking the FTC's 50th Data Security Settlement* (January 31, 2014) http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.
[185] *Id.*

constitutes reasonable data protection.[186] As previously stated, generally speaking the FTC explicitly observes that good data security is a process involving identification of assets and risk, data minimization, a data breach response plan, and physical, technical and administrative safeguards.[187] However, more specifically, a review of the FTC's complaints reveals that what the agency considers unreasonable largely overlaps with several established industry standards such as NIST 800-50 and ISO 27001.[188]

---

[186] FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 2 (2012), available at http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf ("To the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work.").

[187] FEDERAL TRADE COMMISSION, *Commission Statement Marking the FTC's 50th Data Security Settlement* (January 31, 2014) http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf; *see also* Julie Brill, Keynote Address Before the Center for Strategic and International Studies, "Stepping into the Fray: The Role of Independent Agencies in Cybersecurity" (September 17, 2014), https://www.ftc.gov/system/files/documents/public_statements/582841/140917csisspeech.pdf ("The core of the NIST Framework is about risk assessment and mitigation. In this regard, it is fully consistent with the FTC's enforcement framework. One of the pillars of reasonable security practices that the FTC has established through our settlements in more than 50 data security cases is that assessing and addressing security risks must be a continuous process.").

[188] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 619 (2014); Kristina Rozan, How Do Industry Standards for Data Security Match Up with the FTC's Implied "Reasonable" Standards—And What Might This Mean for Liability Avoidance?, IAPP (Nov. 25, 2014), https://privacyassociation.org/news/a/how-do-industry-standards-for-data-security-match-up-with-the-ftcs-implied-reasonable-standards-and-what-might-this-mean-for-liability-avoidance ("The NIST SP 800-53 Rev. 4 came closest to covering the 72 reasonable data security practices expected by the FTC, as inferred from the FTC's complaints. Sixty-six of the 72 expected reasonable practices were recommended in this NIST report. In many instances, the "match" between the expected practice and recommended standard was nearly perfect."); NIST, "Security and Privacy Controls for Federal Information Systems and Organizations" (NIST SP 800-53 Rev.4); International Organization for Standardization (ISO)'s "Information technology--Security techniques--Information security management systems—Requirements" (ISO/IEC 27001:2013); The

Similar FTC deference to the consumer robotics industry is desirable for several reasons. First, deference will help keep the law of consumer robotics from being arbitrary and disconnected from practice. Co-regulatory approaches that use industry standards to form rules are also politically palatable as they are the result of stakeholder consensus.

By definition, industry standards also dictate what is feasible in industry. Thus deference can also keep rules regarding consumer robotics from being overly burdensome. Finally, industry standards are constantly updated, thus deference provides for flexibility. If rules are tethered to industry standards, then a new law need not be passed every time standards change. Laws simply evolve with practice.

Of course, not all potential rules of consumer robotics need be deferential to industry standards. Often, there will be no standard for certain activities or designs. Other times, the industry standard will not adequately protect consumers from harm or deception. Thus deference is no panacea. Yet it remains a useful strategy that the FTC has deployed effectively and could do again with consumer robotics. As previously mentioned, industry standards have already begun to emerge regarding safety and robots with more inevitably on the way.[189]

4. The FTC Can and Should Cooperate with Other Agencies

While I argue that the FTC should take the lead in addressing consumer robotics, the agency should not seek to go it alone. There will be many

---

Council on CyberSecurity's Top 20 Critical Security Controls (CCS CSC), https://www.sans.org/media/critical-security-controls/CSC-5.pdf.

[189] ISO 13482:2014, Robots and robotic devices -- Safety requirements for personal care robots, http://www.iso.org/iso/catalogue_detail.htm?csnumber=53820; ISO 10218-1:2011, Robots and robotic devices -- Safety requirements for industrial robots -- Part 1: Robots, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51330; ISO 10218-2:2011, Robots and robotic devices -- Safety requirements for industrial robots -- Part 2: Robot systems and integration, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=41571; ISO/DTS 15066, Robots and robotic devices -- Safety requirements for industrial robots -- Collaborative operation, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62996,

regulatory bodies whose efforts with respect to consumer robotics be relevant to the FTC. The FTC can and should cooperate with overlapping agencies.

The scope of Section 5 is so broad that it routinely overlaps with other regulatory agencies.[190] One court has stated, "Because we live in 'an age of overlapping and concurring regulatory jurisdiction,' a court must proceed with the utmost caution before concluding that one agency may not regulate merely because another may.'"[191]

The FTC has cooperated with other agencies formally with memorandums of understanding. The agency also cooperates informally though regulator communication or simply by remaining consistent with other regulatory bodies. For example, the FTC has worked with the Food and Drug Administration (FDA) for over forty years regarding certain kinds of advertising for food and drugs.[192] The FTC and HHS often coordinate enforcement actions for violations that implicate both HIPAA and the

---

[190] Woodrow Hartzog & Daniel Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. (forthcoming 2015).

[191] FTC v Ken Roberts Co., 276 F3d 583, 593 (DC Cir 2001), quoting Thompson Medical Co. v FTC, 791 F2d 189, 192 (DC Cir 1986). See also FTC v Texaco, Inc., 555 F2d 862, 881 (DC Cir 1976). See generally FTC v Cement Institute, 333 US 683, 694-95 (1948).

[192] *See* Memorandum of Understanding Between The Federal Trade Commission and The Food and Drug Administration, MOU 225-71-8003, http://www.fda.gov/AboutFDA/PartnershipsCollaborations/MemorandaofUnderstandingMOUs/DomesticMOUs/ucm115791.htm; Thompson Medical Inc. v. FTC, 1986 WL 1275690, 791 F2d 189, 192 ("We find no evidence in the regulatory scheme that Congress has fashioned for over-the-counter medications that the FTC is indefinitely barred from all regulatory authority over drug advertising while the FDA conducts its comprehensive review of drug safety. Nowhere in the case law or in the FTC's grant of authority is there even a hint that the FTC's jurisdiction is so constricted. To the contrary, the cases recognize that ours is an age of overlapping and concurring regulatory jurisdiction."); *see also* Overlapping Authority of FTC, CCH-DCLR P 2010.85 (C.C.H.), 2009 WL 5076333 ("The Federal Trade Commission has jurisdiction to prohibit false labeling and misbranding of food, drugs and cosmetics and other products where the false labeling and misbranding constitutes unfair competition in the purview of Section 5 of the FTC Act") (citing Fresh Grown Preserve Corp. v. FTC (2d Cir. 1942) 125 F2d 917).

FTC Act.[193] The FTC has provided comments for the NHTSA regarding privacy in vehicle-to-vehicle communications.[194]

Agency overlap is not only inevitable, but in this instance, desirable.[195] Scholars have argued that when agencies have overlapping authority, their competition brings them closer to the intent of Congress when granting authority.[196]

Robots are or will soon become involved in many diverse areas such as commerce, aviation, traffic, lodging, healthcare, pharmaceuticals, games, socialization, and many others. Cooperation will be key to ensure consistency, accuracy, and efficiency. Here is where Calo's proposed Federal Robotics Commission could prove the most useful. Calo suggested that one of the functions of the FRC should be to "[a]dvise other federal agencies on matters having to do with robotics, including the DOT on driverless cars, the SEC on high speed trading, the FDA on robotic medical devices, the FCC on cognitive radios, the FAA on drones and, eventually, the Federal Trade Commission on increasingly sophisticated consumer products."[197] Given the FTC's broad authority and history of cooperating with other agencies, it is a strong candidate to take the lead on regulating consumer robotics while cooperating with existing and proposed administrative agencies.

---

[193] Order Denying Respondent LabMD's Motion to Dismiss, In the Matter of LabMD, No. 9357, http://www.ftc.gov/sites/default/files/documents/cases/140117labmdorder.pdf (citing HHS, Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, Final Rule, 78 Fed. Reg. 5566, 5579 (Jan. 25, 2013)).
[194] FTC Provides Comment to NHTSA on Privacy and Vehicle-To-Vehicle Communications, FTC (Oct. 24, 3014), https://www.ftc.gov/news-events/press-releases/2014/10/ftc-provides-comment-nhtsa-privacy-vehicle-vehicle-communications.
[195] Jacob E. Gersen, Overlapping and Underlapping Jurisdiction in Administrative Law, 2006 Sup. Ct. Rev. 201, 208 (2006) ("statutes that parcel out authority or jurisdiction to multiple agencies may be the norm, rather than an exception." and "Because overlapping and underlapping jurisdictional assignment can produce desirable incentives for administrative agencies, statutes [that create overlapping and underlapping jurisdictional schemes] are useful tools for managing principal-agent problems inherent in delegation.").
[196] Jacob E. Gersen, *Overlapping and Underlapping Jurisdiction in Administrative Law*, 2006 SUP. CT. REV. 201, 212 (2006).
[197] Ryan Calo, *The Case for a Federal Robotics Commission*, BROOKINGS (September 2014), http://www.brookings.edu/research/reports2/2014/09/case-for-federal-robotics-commission#ftn12.

CONCLUSION

In many ways, robots are nothing special. Neil Richards and Bill Smart argued, "Robots are, and for many years will remain, tools. They are sophisticated tools that use complex software, to be sure, but no different in essence than a hammer, a power drill, a word processor, a web browser, or the braking system in your car."[198]

Yet robots are unique in utility and social meaning. People rarely name their hammers or have candid conversations with their power drills. A robot can do things hammers never dreamed of. In the same way that paintings do not raise the same privacy problems as digital photographs, robots are unique enough from existing technologies to warrant exceptional legal consideration in some contexts.

The FTC can respond to both exceptional and traditional issues presented by robots. A relatively light regulatory touch for now focused on deception, disclosures, data security, and extreme cases of malicious design will allow consumer robots to flourish while protecting consumers. Consumers want their robots to be safe and truthful. But they do want them. Thus the FTC, or whatever agency ultimately takes the lead on consumer robotics, should seek to find analogs where possible, keep an eye out for genuinely new problems, and otherwise seek to make sure that consumers can continue to buy and use robots in a safe, sustainable way.

[199]

[198] Neil M. Richards & William D. Smart, How Should the Law Think About Robots?, In Proceedings at We Robot 2012, University of Miami, http://robots.law.miami.edu/wp-content/uploads/2012/03/RichardsSmart_HowShouldTheLawThink.pdf.
[199] https://www.flickr.com/photos/decaf/3472018290/ (CC BY-NC-ND 2.0).