12-20-2016

Et tu, Android?: regulating dangerous and dishonest robots

Woodrow Hartzog
Boston University School of Law

Et Tu, Android? Regulating Dangerous and Dishonest Robots

Woodrow Hartzog
Cumberland School of Law, Samford University

Consumer robots like personal digital assistants, automated cars, robot companions, chore-bots, and personal drones raise common consumer protection issues, such as fraud, privacy, data security, and risks to health, physical safety, and finances. They 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.

This paper argues that the FTC's grant of authority and existing jurisprudence are well-suited 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.

Keywords: human-robot interaction, consumer protection, anthropomorphism, automation

1. Introduction

If we are going to make robots part of our daily lives, we might want to watch our backs. Or hair. In 2015, 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. This uncertainly is going to be a problem.

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

1. *See* Matthew Humphries, *Fire department called after robot vacuum 'attacks' sleeping owner*, GEEK (Feb. 6, 2015), 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), 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), http://www.bbc.com/news/26850761; *see also* Satnam Narang, *Tinder: Spammers flirt with popular mobile dating App*. Symantec (July 1, 2013), http://www.symantec.com/connect/blogs/tinder-spammers-flirt-popular-mobile-dating-app

3. *See, e.g.*, Jacqueline Kory Westlund & Cynthia Breazeal, *Deception, secrets, children, and robots: What's acceptable?* 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*, 2011 IEEE International Conference on Systems, Man, and Cybernetics. Retrieved from http://www.cindybethel.com/publications/IEEESMC2011-BethelCL.pdf; Cynthia Breazeal, Designing Sociable Robots (2004); M. Fior et al., *Children's relationships with robots: Robot is child's new friend*, 4 J. Physical Agents 9 (2010).

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.

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 equipped to protect consumers who purchase and use robots? What should the FTC's consumer robotics jurisprudence look like?

The goal of this essay is to explore problems posed consumer robotics and how they might be regulated. I argue that that the FTC's grant of authority and existing jurisprudence make this agency well-suited to protect 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.

2. 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 difficult 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.[7] However, in many ways, robots are exceptional with respect to consumer protection. In a series of articles, Ryan Calo described how robots will challenge 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.[8]

---

4. Neil M. Richards & William D. Smart, *How Should the law think about robots?* We Robot Conference (2012), http://robots.law.miami.edu/wp-content/uploads/2012/03/RichardsSmart_HowShouldTheLawThink.pdf

5. *Id.* at 5.

6. *Id.*

7. 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-businesses are exploiting these applications to garner trust where no such trust is warranted." 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. Ian Kerr, *Bots, babes, and the Californication of commerce*, 1 University of Ottawa Law & Technology Journal, 285-384 (2004).

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?[9] Should software terms of use be subjected to more scrutiny when they govern mechanical body parts like implanted hearing aids and electronic body parts?[10] Should robot salespeople be subject to different rules than their human counterparts?[11] So many questions. Let's begin with a rundown of dubious robots.

2.1. 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 also trust them with our physical well-being.[12] One of the fastest growing segments of robotics is in the field of health care.[13]

Companies are going to make many representations about what robots can and will do. Sometimes the robots themselves will tell us these things. Consumer robotics will only flourish when we can trust that these statements are true. Deception is a classic consumer protection issue.[14] 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. [15] 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]

---

8. M. Ryan Calo, *Robotics and the lessons of cyberlaw*, 103, California Law Review 513 (2015); *see also* M. Ryan Calo, *People can be so fake: A new dimension to privacy and technology scholarship*, 114 Pennsylvania Law Review, 809 (2010); M. Ryan Calo, *Open robotics*, 70 Maryland Law Review 571 (2011); M. Ryan Calo, *Against notice skepticism in privacy (and elsewhere)*, 87, Notre Dame Law Review 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, Eds., 2012).

9. *See* Ryan Calo, *A robot really committed a crime. Now what?* Forbes (Dec. 23, 2014), 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

10. *See* Benjamin Wittes & Jane Chong, *Our cyborg future: Law and policy implications*, Brookings (Sept. 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 *Lessons learned from the identity trail: Anonymity, privacy and identity*, 335 (Ian Kerr, Valerie Steeves, & Carole Lucock, Eds., 2009).

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

12. Calo, *Robots and privacy*, *supra* note 8, at 187, 194.

13. Laurel Riek, Woodrow Hartzog, Don Howard, AJung Moon, & Ryan Calo, *The emerging policy and ethics of human-robot interaction*, 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?* 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 potential for genuine end-user empowerment?* 10th ACM/IEEE Conference on Human-Robot Interaction (HRI) (2015), http://www.openroboethics.org/hri15/wp-content/uploads/2015/02/Hf-Felzmann.pdf

14. *See* Chris Hoofnagle, Federal Trade Commission Privacy Law & Policy (2016).

15. 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.

Letter from James C. Miller III to Hon. John D. Dingell, app. at 175 (1984).

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* International Harvester Co., 104 F.T.C. 949 app. at 1070–76 (1984). Retrieved from https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness

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 notion of robots' capabilities is formed by popular movies, books, and other aspects of pop culture rather than by reality.[17] This makes marketing robots a ripe opportunity for deception because consumers are primed to believe.

For example, one problematic type 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.[18] These videos sometimes speed up the robots' motion 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.[19]

Another area of robotic deployment where deception becomes a problem involves what is known as a "Wizard-of-Oz setup."[20] 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."[21] 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."[22]

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."[23] When would a company's Wizard-of-Oz deployment become a deceptive trade practice? Would it be similar to "pretexting" (pretending to be someone you are not to gain access to information), which the FTC has outlawed?[24] 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.

2.2. 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

17. *See* Richards & Smart, *supra* note 4.

18. I thank Ryan Calo for bringing this problem to my attention.

19. *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 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.'").

20. *See, e.g.*, Laurel D. Riek, *Wizard of Oz studies in HRI: A systematic review and new reporting guidelines*, Journal of Human-Robot Interaction, 1, 119 (2012).

21. *Id.*

22. Westlund & Breazeal, *supra* note 3.

23. *Id.* (citing Breazeal, *supra* note 3); M. Coeckelbergh, *Are emotional robots deceptive?* IEEE Transactions on Affective Computing, 3, 388 (2012)); *see also* David J. Atkinson, *Robot trustworthiness: Guidelines for simulated emotion*, 10th ACM/IEEE Conference on Human-Robot Interaction (HRI) (2015), http://www.academia.edu/9889659/Robot_Trustworthiness_Guidelines_for_Simulated_Emotion

24. Complaint for injunction and other equitable relief, FTC v. Rapp, No. 99-WM-783 (D. Colo. Apr. 21, 1999). Retrieved from http://www.ftc.gov/sites/default/files/documents/cases/1999/04/ftc.gov-touchtonecomplaint.htm

stimulation.[25] 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.[26]

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.[27] One company has marketed "Cheerson," a small a small glider with propellers that can be controlled by a cell phone.[28] 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.[29]

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 if they interact with a robot, their personal information is fair game? Does it matter that some robots are specifically designed to extract personal information through social engineering?

2.3. 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.[30] Humans rely too heavily on available anecdotes and judgments reached by computers.[31] We attribute human emotions and agency to machines.[32] We care too much what others think about us and we increasingly entrench ourselves in opinions formed based on trivial, anecdotal, and arbitrary evidence.[33] 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."[34]

---

25. Calo, *Robots and privacy*, *supra* note 8, at 194; Kristen Thomasen, *Liar liar pants on fire! Examining the constitutionality of enhanced robo-interrogation*, We Robot Conference (2012), http://robots.law.miami.edu/wp-content/uploads/2012/01/Thomasen_CONSTITUTIONALITY-OF-ROBOT-INTERROGATION.pdf; 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

26. Calo, *Robots and privacy*, *supra* note 8, at 187, 194. ("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.")

27. *See, e.g.*, Ryan Calo, *The drone as privacy catalyst*, Stanford Law Review Online, 64, 2 (2011); Gregory S. McNeal, *Alleged drone 'peeping tom' photo reveals perils of drone related journalism*, Forbes (July 14, 2014), 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 (June 24, 2014), http://www.usatoday.com/story/news/nation-now/2014/06/24/seattle-woman-drone-apartment-washington/11339835

28. Cheerson, http://www.cheersonhobby.com/en-US (last visited Oct. 28, 2016).

29. *See, e.g.*, Aspen Way Enters., Inc., F.T.C. File No. 112 3151, No. C-4392 (F.T.C. Apr. 11, 2013); CyberSpy Software, LLC, and Trace R. Spence, F.T.C. 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

30. *See, e.g.*, Daniel Kahneman, Thinking fast and slow (2013); Dan Ariely, Predictably irrational: The hidden forces that shape our decisions (2nd ed., 2009); Daniel Thayer & Cass Sunstein, Nudge: Improvising decisions about health, wealth, and happiness (2nd ed., 2009).

31. *See* Kahneman, *supra* note 30; Daniel Keats Citron, T*echnological due process*, Washington University Law Review, 85, 1249 (2007).

32. *See* Kate Darling, *Extending legal rights to social robots*, We Robot Conference, (2012), http://robots.law.miami.edu/wp-content/uploads/2012/03/Darling_Extending-Legal-Rights-to-Social-Robots.pdf.

33. Kahneman, *supra* note 30; Ariely, *supra* note 30; Thayer & Sunstein, *supra* note 30.

34. Thayer & Sunstein, *supra* note 30; Cass Sunstein, *Nudging: A very short guide*, SSRN, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2499658

In many circumstances, nudging can be acceptable, if not inevitable. But it is not always clear at what point nudging turns to wrongful manipulation. The FTC has a long history of regulating high-pressure sales techniques and otherwise wrongful sales tactics.[35] For example, the agency recently targeted negative-option marketing, whereby "sellers interpret a customer's failure to take an affirmative action, either to reject an offer or cancel an agreement, as consent to be charged for goods or services."[36] Negative-option tactics take advantage of people's noted bias for the status quo.[37]

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 that manipulates humans will impact hundreds, if not thousands or millions of people. Nudgebots are already at work in society. For example, Tinder, the social dating mobile app, has recently been flooded with bots posing as actual users attempting to persuade users to download apps.[38] 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?"[39]

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."[40] 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.[41] As if dating was not complicated enough already.

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.[42] Among other reasons, Darling suggests we might want to protect robots because of the effect robot harm has on humans. We get irrationally attached to them. In fact, even simple household robots like the Roomba vacuum cleaner prompt people to talk to them and develop feelings of camaraderie and gratitude.[43] 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."[44]

---

35. *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) (discussing 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. 22,934, 22,937–38 (1972).

36. FTC, Negative options: A report by the staff of the FTC's division of enforcement (Jan. 2009), https://www.ftc.gov/sites/default/files/documents/reports/negative-options-federal-trade-commission-workshop-analyzing-negative-option-marketing-report-staff/p064202negativeoptionreport.pdf; s*ee also* FTC v. Willms, No. 2:11-cv-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).

37. *See, e.g.*, Cass R. Sunstein, Impersonal default rules vs. active choices vs. personalized default rules: A triptych 9 (May 19, 2013) (unpublished manuscript). Retrieved from http://ssrn.com/abstract_id=2171343 ("In the domain of privacy on the internet, a great deal depends on the default rule.").

38. Leo Kelion, *Tinder accounts spammed by bots masquerading as singles*, BBC (Apr. 2, 2014), http://www.bbc.com/news/26850761

39. *Id*.

40. *Id*.

41. Satnam Nurang, *Tinder: Spammers flirt with popular mobile dating app*, Symantec (July 1, 2013), http://www.symantec.com/connect/blogs/tinder-spammers-flirt-popular-mobile-dating-app?SID=skim38395X1020946X4058df191d7e8584f3eb6715dacc5ed7&API1=100&API2=7104284

42. Darling, *supra* note 30.

43. *Id*.

44. Ryan Calo, *The case for a Federal Robotics Commission*, Brookings (Sept. 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)).

My family owns a Roomba. We named it "Rocco."[45] 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 are feeling and tells us jokes like how much its job "sucks." Over time, our family becomes quite attached to Rocco. One day, poor Rocco starts to sputter along as though sick. It 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.[46] 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?[47] Or what about children, who have difficulty parsing complex emotional attachments and understanding how robots work? Research demonstrates that children can think of a robot as a social being and a friend.[48] Children tell robots secrets that they do not trust with adults.[49] Of course, children also tell secrets to stuffed animals, but mere stuffed animals cannot be programed to extract information or fake emotional bonds via a Wizard-of-Oz setup.

All of these problems are not deal-breakers from consumer robotics. If the law, norms, and the market can temper these possible problems, then consumer robots will be sustainable and help humans flourish. This is why the law should act now to make sure robots can reach their full potential.

3. The FTC is Well-Positioned 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.

3.1. Broad Regulatory Authority

The FTC has a very interesting history.[50] Originally created to combat harmful monopolies, the Wheeler-Lea Amendments to Section 5 of the FTC Act were to prevent "[u]nfair or deceptive trade practices" in addition to

45. *See* Jonathan Coffrey, *What happens when Roomba meets me* (April 24, 2009), https://www.flickr.com/photos/decaf/3472018290 (posting a picture of a mustached and "googly"-eyed Roomba with the assertion, "First of all, ask anybody with a Roomba, it has a name (meet Scruffy, the Janitor)").

46. *Tamagotchi*, WIKIPEDIA, http://en.wikipedia.org/wiki/Tamagotchi (last visited Mar. 18, 2015). Ryan Calo has proposed a similar hypothetical. Ryan Calo, *Could Jibo developer Cynthia Breazeal be the Steve Wozniak of robots?* Forbes (Aug. 17, 2014), http://www.forbes.com/sites/ryancalo/2014/07/17/could-cynthia-breazeal-prove-the-steve-wozniak-of-robots

47. *A robotics companion for the elderly?* GE Ideas 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*, Ethics and Information Technology 14, 27 (2012), http://link.springer.com/article/10.1007/s10676-010-9234-6/fulltext.html

48. Westlund & Breazeal, *supra* note 3.

49. *Id*.

50. *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 (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*, George Washington Law Review, 8, 257 (1939); Eugene R. Baker & Daniel J. Baum, *Section 5 of the Federal Trade Commission Act: A continuing process of redefinition*, Villanova Law Review, 7, 517 (1962).

"unfair methods of competition."[51] 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.[52] Similarly, the FTC's unfairness authority is also far-reaching. [53]

This broad scope is ideal for a regulatory agency in charge of responding to challenges posed by new technologies. 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 harm that falls outside the scope of traditional torts and other regulatory efforts. Although the linchpin of unfairness is harm, the FTC has not limited the type of harm that is necessary to establish a practice as unfair. The harm simply must be substantial.[54] The FTC's broad authority would be particularly useful given that these are still early days for consumer robotics. While many existing laws might cover emergent issues, other problems might fall through the cracks. The breadth of Section 5 allows it to serve as a safety net to nimbly respond to unanticipated problems.

3.2. 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.

3.2.1. 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, disclosures are required whenever they are necessary to prevent a communication or trade practice from being deceptive.[55] Disclosures must be clear and conspicuous.[56] The agency has detailed specific rules regarding what constitutes effective notice.[57] The FTC also looks to repetition, the use of multiple media for communications, and whether

---

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

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

53. 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 would not quickly become outdated or leave loopholes for easy evasion." FTC Policy Statement on Unfairness, Appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984); *see* 15 U.S.C. § 45(n) (2012).

54. FTC Policy Statement on Unfairness, Appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984) ("First of all, the injury must be substantial. The Commission is not concerned with trivial or merely speculative harms."); *see* 15 U.S.C. § 45(n) (2012).

55. .com disclosures: How to make effective disclosures in digital advertising, FTC (March 2013), https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf

56. *See, e.g.*, 16 CFR § 14.9 (2014) ("clear and conspicuous" disclosure must be made in the language of the target audience); Donaldson v. Read Magazine, Inc., 333 U.S. 178 (1948); .com disclosures, *supra* note 55.

57. 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?

there were distracting factors that might diminish the effectiveness of a disclosure, particularly online.[58] The FTC has also developed nuanced theories regarding deception by omission, use of scientific data, and endorsements.[59] Additionally, the FTC is also not bound by the fine print, which will keep harmful terms that nobody reads from being enforceable.[60]

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' robots 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 toward 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 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 FTC might eventually issue new guidance for robot disclosures as it did with disclosures on the internet.[61]

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. However, new technologies open up opportunities for innovative new forms of notice. Ryan Calo has proposed a policy shift toward "visceral notice," that is, "[leveraging] a consumer's very experience of a product or service to warn or inform."[62] Could 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." They can mimic human emotion for a more intuitive version of notice. For example, a robot can yell at people or look them directly in the eyes and speak in a stern voice. It seems this would be more likely than dense, unreadable text. Since robots can mimic conversation, they can also follow up to make sure people have understood the notice.

.com disclosures, *supra* note 55; *see also* Donaldson v. Read Magazine, Inc., 333 U.S. 178 (1948); Decision and Order, BUY.COM, Inc., C-3978 (Sept. 8, 2000). Retrieved from https://www.ftc.gov/sites/default/files/documents/cases/2000/09/buydotcom.do.pdf; Hewlett-Packard Co., File No. 002-3220 (April 3, 2001), https://www.ftc.gov/sites/default/files/documents/cases/2001/04/hpagr.htm (proposed consent agreements published for public comment); Microsoft Corp., File No. 002-3331 (April 3, 2001) https://www.ftc.gov/sites/default/files/documents/cases/2001/04/msagr.htm (same); Häagen-Dazs Co., 119 F.T.C. 762 (1995) (Consent Order).

58. *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).

59. *See* Thusnet & Goldman, *supra* note 18.

60. *See, e.g.*, Consent Order, BUY.COM, Inc., FTC No. 992 3282, C-3978 (Sept. 8, 2000). Retrieved from https://www.ftc.gov/sites/default/files/documents/cases/2000/09/buydotcom.do.pdf; Consent Order, Hewlett-Packard Co., File No. 002-3220 (April 3, 2001); Consent Order, Microsoft Corp., File No. 002-3331 (April 3, 2001); Tushnet & Goldman, *supra* note 18 ("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.").

61. .com disclosures, *supra* note 55.

62. M. Ryan Calo, *Against notice skepticism in privacy (and elsewhere)*, *supra* note 8, at 1030.

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

3.2.2. 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, design-based solutions are attempts to create or modify a technology, architecture, or organizational structure or procedure *ex ante* as an attempt to reduce the likelihood of harm. Design-based solutions are at the heart of the "privacy by design" movement that seeks to "bake privacy in" to products and business processes.[63]

Design-based solutions are prospective and implicitly embrace a probabilistic notion of protection. In most circumstances, they make consumer harm less likely 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 activity so high that most potential third-party bad actors simply would not 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 harder 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. In several complaints, the agency deemed software unfair because of its malicious nature that was difficult for consumers to recognize or retaliate against. For example, the FTC found that unexpected default software settings that shared a user's information without their knowledge were unfair.[64] In addition, the FTC developed a theory of culpability for design choices that indirectly harm consumers.[65] For example, providing the means and instrumentalities to install spyware and access customer's personal information is considered an unfair trade practice.[66]

The FTC only occasionally pursues 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.[67] Should home care robots be

63. *Privacy by Design*, Information Commissioner's Office, https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design ("Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. Unfortunately, these issues are often bolted on as an after-thought or ignored altogether."); Ann Cavoukian, *Privacy by Design*, https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-primer.pdf (last accessed October 28, 2016).

64. Decision and Order, Sony BMG Music Entertainment, FTC File No. 062 3019, No. C-4195, at 6 (June 29, 2007). Retrieved from http://www.ftc.gov/sites/default/files/documents
cases/2007/06/0623019do070629.pdf; Press release, FTC, Android flashlight app developer settles FTC charges it deceived consumers (Dec. 5, 2013), http://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived; Complaint for permanent injunction and other equitable relief at 13, FTC v. Frostwire, LLC, No. 11-cv-23643 (S.D. Fla. Oct. 12, 2011). Retrieved from http://www.ftc.gov/os/caselist/1123041/111011frostwirecmpt

65. DesignerWare, LLC, FTC File No. 112 3151, No. C-4390 (Apr. 11, 2013). Retrieved from http://www.ftc.gov/sites/default/files/documents/cases/2013/04
130415designerwarecmpt.pdf; Complaint, FTC v. Neovi, Inc., No. 306-CV-01952-WQH-JMA (S.D. Cal. Sept. 19, 2006). Retrieved from https://www.ftc.gov/sites/default/files/documents/cases/2006/10
060919neovicmplt.pdf

66. Complaint at 10–11, FTC v. CyberSpy Software, LLC and Trace R. Spence, No. 6:08-CV-01872 (M.D. Fla. Nov. 5, 2008). Retrieved from https://www.ftc.gov/sites/default/files/documents/cases/2008/11/081105cyberspycmplt.pdf

designed to record private moments like going to the bathroom? Should robots be programmable or controllable by anyone, or just by 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?[68] Or can companies design robots to be "open" without incurring liability, in the sense that they have a non-dedicated use, nondiscriminatory software, and modular design?[69]

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.

3.2.3. 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 engage in involving identification of assets and risks, data minimization, implementation of administrative, technical, and physical safeguards, as well as the development of a data breach response plan.[70] But, at base, it is a component necessary to build consumer trust.

The FTC has established robust data security jurisprudence, filing over fifty data security complaints in the past fifteen years that obligate companies collecting and storing personal information to provide reasonable data security requirements.[71] 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.[72]

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..[73] 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 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."[74] According to the FTC, "[t]he 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."[75]

---

67. *See generally* Robot ethics: The ethical and social impications of Robotics, 187, 194 (Patrick Lin, Keith Abney & George A. Bekey, Eds., 2012); Riek et al., *supra* note 13; Calo, *Open robotics*, *supra* note 8; Aimiee Van Wynsberghe, *A method for integrating ethics into the design of robots*, Industrial Robot: An International Journal, 433, (2013); Aimiee Van Wynsberghe, *Designing robots for care: Care centered value-sensitive design*, Science and Engineering Ethics, 19, 407 (2013).

68. *See* Calo, *Open robotics*, *supra* note 8.

69. *Id.*

70. *Commission statement marking the FTC's 50th data security settlement*, FCT (January 31, 2014) http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf

71. Complaint, TRENDnet, FTC No. 122 3090, No. C-4426 (Feb. 7, 2014). Retrieved from https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf

72. *See, e.g.*, Complaint, BJ's Wholesale Club, Inc., 140 F.T.C. 465, 468 (2005). Retrieved from https://www.ftc.gov/sites/default/files/documents/cases/2005/09/092305comp0423160.pdf; Complaint, TRENDnet, FTC No. 122 3090, No. C-4426

73. Complaint at 5, TRENDnet, FTC No. 122 3090, No. C-4426

74. FTC, Protecting Consumer Privacy Act in an era of rapid change: Recommendations for business and policymakers, 2 (2012). Retrieved from http:// www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

75. *Id.*

The FTC even requires companies to implement privacy by design in its consent orders through a "comprehensive privacy program."[76] 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 adjustments of the program.[77] Processes like these could also work for companies that design robots, particularly those that collect personal information.

4. Conclusion: The FTC Should Take the Lead on Regulating Consumer Robotics

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."[78]

However, 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 focused on deception, disclosures, data security, and extreme cases of malicious design will allow consumer robots to flourish for now, while protecting consumers. Perhaps most importantly, the FTC can take this opportunity to embrace the incredible literature in the field of human-robot interaction (HRI) to inform its efforts.[79] People interact with and react to robots in unique and complex ways. Regulatory efforts for HRI will only be successful if they are compatible with the latest research.

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 consumers can continue to buy and use robots in a safe, sustainable way.

Acknowledgements

The author would like to thank Ryan Calo, Danielle Citron, Kate Darling, Brannon Denning, Evan Selinger, Michael Froomkin, Margot Kaminski, the participants of the We Robot 2015 Conference, and the staff of the Maryland Law Review. The author would also like to thank Megan Fitzpatrick and Lydia Wimberly for their excellent research assistance. A longer version of this essay appeared in the Maryland Law Review titled "Unfair and Deceptive Robots."

W. Hartzog, Samford University's Cumberland School of Law, Birmingham, AL, USA. Email: whartzog@samford.edu

76. Consent Order, Snapchat, FTC No. 132 3078 (May 8, 2014). Retrieved from https://www.ftc.gov/system/files/documents/cases/140508snapchatorder.pdf
77. *Id.*
78. Richards & Smart, *supra* note 4.
79. Michael A. Goodrich and Alan C. Schultz, *Human-robot interaction: A survey*, Foundations and trends in human-computer interaction, 1, 203 (2007).