Idaho Law Review

Volume 51 | Number 3 Article 4

March 2019

Robots in the Home: What Will We Have Agreed To?

Margot E. Kaminski

Follow this and additional works at: https://digitalcommons.law.uidaho.edu/idaho-law-review

Recommended Citation

Margot E. Kaminski, *Robots in the Home: What Will We Have Agreed To?*, 51 Idaho L. Rev. 661 (2019).
Available at: https://digitalcommons.law.uidaho.edu/idaho-law-review/vol51/iss3/4

This Article is brought to you for free and open access by Digital Commons @ UIdaho Law. It has been accepted for inclusion in Idaho Law Review by an authorized editor of Digital Commons @ UIdaho Law. For more information, please contact annablaine@uidaho.edu.

ROBOTS IN THE HOME: WHAT WILL WE HAVE AGREED TO?

MARGOT E. KAMINSKI*

TABLE OF CONTENTS

I. INTRODUCTION

A new technology can expose the cracks in legal doctrine. Sometimes a technology resists analogy. Sometimes through analogies, it reveals inconsistencies in the law, flaws in framing, or friction in the fit between different parts of the legal system. This essay addresses robots in the home, and what they reveal about U.S. privacy law. Household robots might not themselves destroy U.S. privacy law, but they will reveal its inconsistencies, and may show where it is most likely to fracture. Just as drones are serving as a legislative "privacy catalyst"[1]—encouraging the enactment of new privacy laws as people realize they are not legally protected from privacy invasions—household robots may serve as a doctrinal privacy catalyst.

* Assistant Professor of Law at the Ohio State University Moritz College of Law, and Affiliated Fellow at the Information Society Project at Yale Law School. Thanks to Jack Balkin for co-teaching our Artificial Intelligence and Robots seminar, Ryan Calo for welcoming me into the law-and-robotics community, and Bryan H. Corbellini for giving me a much-needed afternoon off. Thanks to Scott Peppett and Guy Rub for helpful comments. Mistakes are my own.

1. Ryan Calo, *The Drone as Privacy Catalyst*, 64 STAN. L. REV. ONLINE 29, 29–33 (2011).

Household robots may spur doctrinal changes by virtue of a number of their technosocial characteristics.

Some household robots are already here: the Roomba already vacuums our floors and scares our pets. In Japan, fuzzy robot seals are used in eldercare.[2] Robots may come into the home first as toys. Mattel is touting its speaking doll, "Hello Barbie," and the robotic dinosaur toy, Pleo, uses speech recognition and adapts to its owner's behavior.[3] Household and caretaker robots are on the agenda for major technology companies. Bill Gates in 2007 called for a "robot in every home . . . ."[4] And Toyota is currently experimenting with "care assist robots" that can lift and carry elderly patients, preventing injury to human caretakers and allowing people with dementia to remain longer in their homes.[5] *Robot & Frank*, an only slightly futuristic movie about an elderly man with a friendly caretaker robot, envisions a near future in which privacy, ethics, and relationships are challenged by a helpful household robot.[6]

There are two basic legal puzzles raised—or revealed—by household robots. First, there is the question of whether a robot's permission to be in a space also grants it permission to record information about that space. Second, there is the broader legal question of whether traditional legal protection of the home as a privileged, private space will withstand invasion by digital technology that has permission to be there. In other words, when we agree to allow robots in our homes, are we correspondingly agreeing to allow them to record? To allow in the third parties with which robots communicate? This essay's basic claim is that the legally salient aspects of home robots may drive a collision between the doctrinal understanding of privacy in real physical space, and privacy in the digital realm. That conflict in turn reveals inconsistent understandings of permission and consent in context, across privacy law.

This essay begins by identifying the legally salient features of home robots: the aspects of home robots that will likely drive the most interesting legal questions. It then explores how current privacy law governing both law enforcement and private parties addresses a number of questions raised by home robots. First, how does privacy law treat entities that enter places (physically, or through sense-enhancing technologies) where they are not invited? Second, how does privacy law treat entities that *are* invited into a physical space, but were not invited to *record* in that space? How does privacy law treat consent, both express and implied? Fourth, how does privacy law address entities that lull—or deceive—people into revealing more than they intend to? And finally, in the private actor context, will robotic recording be considered to be speech?

---

2. Andrew Griffiths, *How Paro the Robot Seal is Being Used to Help UK Dementia Patients*, GUARDIAN (July 8, 2014, 9:01 AM), http://www.theguardian.com/society/2014/jul/08/paro-robot-seal-dementia-patients-nhs-japan.

3. *Barbie Doll Will Be Internet Connected to Chat to Kids*, BBC NEWS (Feb. 17, 2015), http://www.bbc.com/news/technology-31502898; *For Pleo the Robot Dinosaur, a Second Act in an American Life*, CNET (January 9, 2014, 4:00 AM), http://www.cnet.com/news/for-pleo-the-robot-dinosaur-a-second-act-in-an-american-life/.

4. *See* Bill Gates, *A Robot in Every Home*, SCI. AM., January 2007, at 58, 65, *available at* http://www.cs.virginia.edu/~robins/A_Robot_in_Every_Home.pdf.

5. Wendy Hall, *Technology Could Help People With Dementia Remain in Their Homes*, GUARDIAN (June 23, 2014, 3:30 AM), http://www.theguardian.com/social-care-network/2014/jun/23/technology-help-people-dementia-longitude-prize.

6. ROBOT & FRANK (Samuel Goldwyn Films 2012).

The rise of robots in the home is a form of technosocial change.[7] Both the technology and the social norms around its use will develop. That technosocial change in turn will reveal strains in the law's treatment of privacy harms, especially around questions of what constitutes sensitive information, and the role of consent or assumption of risk.

Evaluating how home robots might be treated under U.S. privacy law leads to at least one particularly interesting observation: that U.S. privacy law's treatment of the government and treatment of private actors are not aligned with respect to the voluntary sharing of information by a data subject. In the Fourth Amendment context, sharing information with a third party gives rise to an assumption of risk that law enforcement might access that information—and thus means law enforcement may access that information without a warrant. In the private actor context, however, sharing information with a third party gives rise to obligations on behalf of that third party to protect the information.

This essay also contributes the observation that the legally interesting aspects of a new technology will vary depending on what kind of law is applied. What is interesting about a technology from the perspective of, say, tort law or tax law is not necessarily interesting from the perspective of privacy law. This observation responds to Ryan Calo's recent discussion of why robots are or are not exceptional.[8] A technology and it social uses may be exceptional in different areas of law for different reasons—and may simultaneously be completely unexceptional elsewhere.

II. WHY HOUSEHOLD ROBOTS ARE LEGALLY INTERESTING

Robots are embodied technologies that contain software, or code, and move and act on other objects in real space. While there is no single definition of a robot, some consensus has formed around defining robots as technologies that sense, think, and then act on and in the physical world.[9] The Internet of Things and household robots raise privacy questions along the same spectrum, but certain features of robots—that they can move by themselves, may make their "own" decisions, and have social meaning—will raise fairly unique privacy questions.

The technical definition of what a robot is differs from what might make a robot interesting from a legal perspective. This section thus addresses legally salient aspects of household robots: the aspects that are particularly of interest to privacy law. To identify the legally salient features of household robots, we must start with (1) the privacy harms at issue, and (2) why implied consent or assumption of risk is central to the legal discussion.

A. Types of Privacy Harm

To understand what aspects of household robots are legally salient, we have to articulate what privacy harms household robots might cause. Robots, as part of their basic functionality, sense and record their environment. They will often share that

7. Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 619 (2011) (using the term "technosocial" to refer to the "intertwined effects of technological and social change").

8. Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. (forthcoming 2015), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2402972.

9. *Id.* at 117.

information with third parties, or store that information in the cloud. Household robots thus pose two basic privacy concerns: concerns over the excessive sharing and processing of information, and concerns over the initial recording of information.

Information sharing can threaten contextual integrity: the reliance people place on the idea that information revealed in one context, governed by one set of social norms, will not be moved into or used in another.[10] The sharing of information gathered by household robots would take information revealed in the home, and share or use it in very different contexts.[11] This type of privacy violation could cause chilling and conforming effects. When information revealed in the home is shared and used outside of the home, people may stop trusting that the home is a private location, and may stop sharing information and conform their behavior to majority norms even within the home.[12]

A second, related type of privacy harm threatened by household robots occurs at the moment at which information is captured.[13] The second type of privacy harm that household robots threaten is to interfere with individual's ability to accurately dynamically manage social accessibility at a particular moment, by capturing information people assume will not be captured. People often use physical features of their environment, such as walls, to manage their social accessibility. They also rely on features of social relationships—the idea that a trusted person will not disclose information to third parties—and on temporal features of relationships, such as forgetfulness over time. Household robots threaten the ability of individuals to conduct this "boundary management" because in addition to crossing physical boundaries, or being able to "sense" through physical boundaries using sense-enhancement technologies, robots' social features may elicit trust where trust is not deserved. Thus household robots pose at least two harms with respect to information capture: people may inaccurately manage their social accessibility, or knowing that they are watched, may again change their behavior at the moment of interaction.

B. Consent or Assumption of Risk

A recurring theme in U.S. privacy doctrine is that in certain contexts, by disclosing information people assume the risk that information will travel, and thus cannot claim that their privacy has been violated.[14] For example, two people embracing at a fair could not claim that their privacy had been violated when a photograph of the embrace ended up on the front page of a newspaper, because they assumed the risk the information would travel by embracing in a public space.[15] And under the Fourth Amendment, you currently have no reasonable expectation of privacy in the

10. *See* Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 L. & PHIL. 559, 567–68 (1998), *available at* http://www.nyu.edu/projects/nissenbaum/papers/privacy.pdf.

11. *See generally* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004).

12. *See generally* Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465 (2015).

13. Margot E. Kaminski, *Theory of Privacy for Information-Gathering Laws*, WASH. L. REV. (forthcoming) (on file with author).

14. *See generally* Gill v. Hearst Publ'g Co., 253 P.2d 441 (1953).

15. *Id.*

phone numbers you dial, in part because you share them with the telephone company.[16] Perhaps the biggest doctrinal puzzle raised by household robots will be whether information revealed in a traditionally private location—the home—can be treated as not private because it has been shared with third parties as a part of a robot's functioning.

C. The Legally Salient Aspects of Household Robots

As discussed, household robots may cause two types of privacy harms: violation of contextual integrity and boundary management challenges. Whether those privacy harms will be legally protectable may hinge on whether people are understood to be assuming a risk of privacy violations by sharing information with third parties. This understanding gives us the background for identifying the legally salient aspects of household robots.

Ryan Calo has suggested that robots in general will have three effects on privacy: they will increase the amount of direct surveillance, they will increase access to formerly private spaces, and they will have social meaning.[17] Calo has also suggested more generally that the "essential qualities" of robots—which I understand to be the legally salient qualities of robots—are (1) embodiment, (2) emergence, and (3) social valence.[18] This essay takes a narrower approach, asking what aspects of household robots in particular are legally salient, from the perspective of privacy law. Interestingly, taking this narrower approach reveals slightly different salient features. This suggests that what is legally salient about a new technology will depend on which laws are applied.

The **ability of robots to sense and record information**, and likelihood that they will **share that information with third parties** for storage and processing purposes, are clearly legally salient features from a privacy perspective. On the one hand, the fact that robots must take in information to properly navigate an environment (just as a phone call must be made on telephone lines) suggests that the sensing might be treated as necessary for functionality and deserving of legal privacy protection. On the other hand, the known ability of robots to record massive amounts of information about private places raises the question of whether household robot owners have consented to that recording, implicitly or explicitly, by having a robot in the home.

The sensory aspect of robots also raises interesting legal questions about how to treat a robot (1) that records more information than is necessary for functionality; (2) that records more information than it has told its owner it is recording (fails to provide notice); (3) that has been given permission to enter or operate in certain locations, but not to record in those locations; and (4) that senses or records information humans aren't used to monitoring with their own senses (like temperature). The centrality of sensing and recording to household robots' functionality is a legally salient aspect of household robotics, especially when that sensing involves non-visual senses such as thermal imaging.

---

16. *See generally* Smith v. Maryland, 442 U.S. 735 (1979).

17. M. Ryan Calo, *Robots and Privacy*, *in* ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS 187, 187–88 (Patrick Lin, Keith Abney & George A. Bekey eds., 2012).

18. Calo, *supra* note 9 (manuscript at 120–36).

The **ability of household robots to move and otherwise interfere with their physical environments** is a second legally salient feature. If a robot can open doors, or go into rooms of a house where it has not been invited, it is capable of violating contextual integrity or threatening boundary management. But if a person fully understands that their household robot is capable of going wherever it wants, then the known ability of robots to move from room to room or through doors may suggest that the robot's owner has assumed the risk that the home is no longer private. Thus movement is one legally salient feature of household robots: depending on how courts characterize it, movement could push the legal doctrine in a number of directions.

The **social valence or social meaning** of home robots—that is, the fact that robots may be anthropomorphic or appear as quasi-human actors—will be salient to privacy law. There is evidence that people treat anthropomorphic robots with increased compassion and trust.[19] A robot that lulls people into revealing more than they intend to may be viewed as deceptive technology; or it may be treated similarly to false human friends.

Finally, the **ability of robots to process information**, or "think" and "make decisions," is legally salient. Emergent behavior could affect the scope of implied consent or assumption of risk if household robots make decisions outside the scope of what their owners believe they have agreed to. It may also affect discussions of what kind of liability regime should be in place for robot creators, influencing discussion of whether there should be a strict liability regime or negligence standard, or something else. Finally, emergent behavior will affect legal conversations about the applicability of the emerging First Amendment right to record, and whether robots—or their programmers—should be legally considered to be "authors" of the recorded information they gather.[20]

In summary, the legally salient aspects of household robots include: (1) their need to sense and ability to record vast amounts of information that they often will share with third parties; (2) their ability to independently move in a physical environment; (3) what Calo calls their "social valence" or anthropomorphic characteristics; and (4) their ability to process information, or "think," in complex, unpredictable ways. Of Calo's named qualities of robots, embodiment is less important to privacy law, except as it affects the ability to move through physical space or creates a social presence through anthropomorphic characteristics.

III. WHAT HOUSEHOLD ROBOTS REVEAL ABOUT PRIVACY LAW

This section turns from household robots themselves to what they reveal about U.S. law. New technologies are often incorporated into case law by analogy.[21] But trying to fit household robots into existing boxes under current case law reveals problems and inconsistencies in privacy doctrine. This section begins by discussing

19. Calo, *supra* note 9 (manuscript at 132, 135).

20. Jane R. Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 61 (2014); *see also* Annemarie Bridy, *Coding Creativity: Copyright and the Artificially Intelligent Author*, 5 STAN. TECH. L. REV. 1, 22 (2012) (for discussion of AI authorship in copyright law).

21. Neil M. Richards & William D. Smart, *How Should the Law Think About Robots?* 19 (2013) (prelimary draft), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2263363.

household robots and the Fourth Amendment, and then turns to law governing private actors rather than the government.

A. Government and the Fourth Amendment

The home is privileged in Fourth Amendment analysis; it receives "paramount" privacy protection.[22] The "very core" of the Fourth Amendment is "the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[23] In some ways, U.S. privacy jurisprudence treats "information revealed in the home" as its own category of sensitive information.[24]

But the third party doctrine in Fourth Amendment jurisprudence explains that when people voluntarily share information with third parties, they do not have a reasonable expectation of privacy in that information.[25] Other cases suggest that a person has no reasonable expectation of privacy from a privacy-invading technology that is in general or regular public use.[26] Will the centrality of the home in Fourth Amendment jurisprudence withstand the incursion of household robots? The answer to this question depends in large part on the power of analogies, and on how far courts are willing to extend current understandings about assumptions of risk or implied consent to information gathered in the home.

This Section outlines relevant Fourth Amendment case law on the following questions: first, how might home robots be treated when they enter or observe physical spaces to which they have not been invited? Second, how might home robots be treated when they record information in a location where they have been invited to be—but in which they were not invited to record? Third, how might the presence of home robots be understood to imply consent to the reuse of information? Fourth, how might actual contractual agreements and/or privacy policies around home robots be treated, under the Fourth Amendment? And fifth, how might Fourth Amendment doctrine treat falsely reassuring or outright deceptive robots?

1. Entering where not invited

Household robots might enter a physical space in a home to which they have not been invited, or use sense-enhancing technology to "see" into that space. The legally salient features of household robots with respect to this question are their ability to move, to sense using sense-enhancing technology, and possibly the ability to make emergent decisions that cause them to act "independently," or contrary to owners' preferences.

---

22. Kyllo v. United States, 533 U.S. 27, 31 (2001).

23. *Id.* (citing Silverman v. United States, 365 U. S. 505, 511 (1961)).

24. Sensitive information receives more privacy protection. *See* Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. (forthcoming 2015). For a discussion of how the home is treated as sensitive in Fourth Amendment doctrine, see Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. (forthcoming 2016) (manuscript at 32).

25. *E.g.*, Smith v. Maryland, 442 U.S. 735, 742 (1979).

26. *See generally Kyllo*, 533 U.S. 27 (2001); Florida v. Riley, 488 U.S. 445, 455 (1989) (O'Connor, J., concurring) (asking whether "the observation cannot be said to be from a vantage point generally used by the public . . . ."); California v. Ciraolo, 476 U.S. 207 (1986).

Fourth Amendment jurisprudence once was "tied to common-law trespass," although it did not require technical trespass, only "actual intrusion into a constitutionally protected area."[27] The Supreme Court famously decoupled Fourth Amendment violations from trespass in *Katz v. United States*, explaining that the Constitution "protects people, not places."[28] A person's privacy could be protected in an area outside the home and accessible to the public if the person had a reasonable expectation of privacy.[29] But the Supreme Court also observed in *Katz* that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[30]

The question thus is as follows: when a person lets a robot into her house, and assumes it will remain in one area of the house, is it a violation of that person's reasonable expectation of privacy for the robot to enter, or use sense-enhancing technology to virtually enter, a room or space where it is not supposed to be? To bring this discussion into the scope of the Fourth Amendment, this question presumes that the robot is either controlled or accessed by law enforcement.

The Supreme Court addressed a related question when it evaluated police use of sense-enhancing technology in *Kyllo v. United States*.[31] There, the Court concluded that police could not use thermal imaging to "see" into the interior of the home without a warrant.[32] The majority analogized thermal imaging to trespass, rather than to gathering information such as smells, which could be picked up remotely by humans without technological aids.[33] The Court explained that "obtaining by sense-enhancing technology any information regarding the home's interior that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' constitutes a search—at least where (as here) the technology in question is not in general public use."[34]

The question, then, may be whether police access to information obtained by a robot in searches unauthorized by a homeowner constitutes use of "technology . . . in general public use."[35] Many people may end up with household robots, which may make the robots themselves technology in general public use. But it seems unlikely that people will generally access information from each other's robots, suggesting that government coopting of household robots' ability to move from room to room or see through walls would not involve technology in general public use.

However, three cases on aircraft photography may cut the other way. In *California v. Ciraolo* and *Florida v. Riley*, the Supreme Court found that no warrant is required for law enforcement to employ naked-eye observation or aerial photography from a fixed-wing aircraft, or from a helicopter.[36] In a third case, *Dow Chemical v. United States*, the Court found that enhanced aerial photography did not require a

27. *Kyllo*, 533 U.S. at 31; *Silverman*, 365 U.S. at 510–12.
28. Katz v. United States, 389 U.S. 347, 351 (1967).
29. *See id.*
30. *Id.* at 351.
31. *Kyllo*, 533 U.S. at 31.
32. *Id.* at 40.
33. *Id.* at 48.
34. *Id.* at 28 (citation omitted).
35. *Id.*
36. California v. Ciraolo, 476 U.S. 207, 213–14 (1986); Florida v. Riley, 488 U.S. 445, 445 (1989).

warrant.[37] The Court reasoned that planes and helicopters are common technologies, and thus people do not have a reasonable expectation of privacy against observations made from them. If robots become truly ubiquitous, like planes, then these cases suggest the Fourth Amendment might not offer protection—even if robots have not been granted express permission to be in a particular room or space.

In recent cases, however, the Court has employed preservationist reasoning to protect a level of privacy available before the development of new technologies.[38] In both a recent case on searching cellular telephones, and in *Kyllo*, the Court referred to the necessity of preserving the degree of privacy protection in existence at the time the Fourth Amendment was adopted.[39] If this is truly a guiding principle for the Court, then information gathered by nosy, trespassing robots from the home should remain protected by the Fourth Amendment, regardless of how common robots become.

2. Recording where they are invited to be, but not to record

A second Fourth Amendment question is how to treat robots that are invited into private spaces, but *not invited to record* or observe using another sense. In other words, people may expect household robots to move around in a space, and to perform an expected function, but not to record interactions or share them with other parties.

A recent Supreme Court case can be understood as applicable to this scenario. The Court recently considered whether a drug-sniffing dog brought by police officers onto a porch violated the Fourth Amendment.[40] The Court reasoned that while a police officer may rely on an "implicit license" to walk on the porch to knock at the front door like other visitors, that "implicit license" did not extend to using a trained drug-sniffing dog.[41]

This case suggests that if a household robot has been invited to a private space (ie has a license to be there), but a person can exhibit a real expectation that the robot would not be recording information or using sense-enhancing technology without notice, that person might have a reasonable expectation of privacy against the unpermitted recording.

3. Implied Assumption of Risk (or Implied Consent)

Both of the previous two scenarios involved a robot breaching its owner's orders. In the above two scenarios, a household robot exceeds explicit permissions or ignores an explicit ban by (a) entering (physically or sensually) into spaces unwelcomed, or (b) recording unwelcomed in a space where it might be permitted to phys-

37. Dow Chemical v. United States, 476 U.S. 227, 239 (1986).

38. *See Kyllo*, 533 U.S. at 27–28; *Riley*, 488 U.S. at 445; *see also* Orin Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 426, 489–99 (2011).

39. *Kyllo*, 533 U.S. at 28 ("This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."); Riley v. California, 134 S.Ct. 2473, 2494–95 (2014).

40. Florida v. Jardines, 133 S.Ct. 1409, 1413 (2013).

41. *Id.* at 1415.

ically be. But what about when a robot's owner cannot claim to have denied permission to the robot, either to access specific areas or to record that environment? This is where the doctrinal muddle in Fourth Amendment law revealed by household robots—the tension between third party doctrine and protection for the home—gets most interesting.

Most robots will share information with third parties for processing purposes or just to store information in the cloud. The Supreme Court has in a line of cases explained that people do not have a reasonable expectation of privacy in information, such as the records of phone numbers dialed, revealed to or stored with third parties.[42] If a person fails to restrict their household robot's access to particular parts of the house, or cannot indicate that she thought the robot wasn't recording, then information gathered by the robot and sent to the cloud or revealed to the robot's seller would likely fall within third party doctrine. Then police may access that information through the third party without a warrant. To be clear: there are complex statutory schemes in place for handling police access to stored communications and telephone numbers dialed.[43] But these statutes apply to communications, and thus likely do not apply to most information robots will store.

Justice Sotomayor recently suggested that the third party doctrine has no place in our digital world, since most information is now stored with or communicated through third parties.[44] In a recent decision on cell phone searches, Chief Justice Roberts suggested (but did not hold) that people could have an expectation of privacy in phone numbers when that information is combined with more sensitive information such as labeling a particular number with a name, or "home."[45] These indicators suggest that members of the Court are getting ready to reconsider third party doctrine, or at least to considerably narrow its scope. Similarly, a recent D.C. Circuit decision evaluating the constitutionality of the government's bulk storage of telephone metadata explained that big data is different in kind from the information at issue when the Supreme Court first created the third party doctrine.[46]

Household robots may place the third party doctrine in an even rockier position. Part of the reasoning that gives rise to the third party doctrine is that the information at issue is not inherently sensitive—in the case of phone numbers, it is considered to be "envelope" rather than "content" information.[47] When household robots record information in the home, courts may find that information about the home is inherently more sensitive than "envelope" information like phone numbers, and thus refuse to apply the third party doctrine. We can see this happening in at least two places: first, the Sixth Circuit has held that there is a reasonable expectation of privacy in the content of one's email, even though people technically share their email

42. Smith v. Maryland, 442 U.S. 735, 745 (1979).

43. *E.g.* Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2701 (2014); Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2014); Pen Registers and Traps, 18 U.S.C. § 3121 (2014).

44. United States v. Jones, 132 S.Ct. 945, 957 (2012) (Sotomayor, J., concurring).

45. Riley v. California, 134 S.Ct. 2473, 2490 (2014).

46. Klayman v. Obama, 957 F. Supp. 2d 1, 28 (D.D.C. 2013); *but see In re* FBI, 2013 WL 5741573 (FISA Ct. 2013).

47. *See, e.g.*, Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2113–2117 (2009). *But see* United States v. Miller, 425 U.S. 435, 444 (1976) (treating bank records as "less sensitive" information because the records perform an act [transaction], not because they are envelope information).

with third parties such as Google.[48] Second, the Eleventh Circuit has pointed out that location information in the home is sensitive information[49]—even though location information outside of the home was held in older Supreme Court cases not to be inherently sensitive information.[50] So there is developing precedent for the idea that being in or from the home makes information sensitive in nature.[51]

4. Actual (Contractual) Agreements/ Privacy Policies

One of the more interesting questions that might arise around the sharing of information with third parties by household robots is the impact of an actual agreement—for example, a privacy policy—on a person's "reasonable expectation of privacy." If a person has a robot in their home, and has agreed to a particularly permissive privacy policy, can they still have a reasonable expectation of privacy against the revelation of that information to the government?

The Sixth Circuit addressed this question in its email case.[52] The court reasoned that while some subscriber agreements might be "sweeping enough to defeat a reasonable expectation of privacy … we doubt that will be the case in most situations."[53] Importantly, the Sixth Circuit held that the ability of the third party to access sensitive information—in that case, the contents of emails—does not abolish an expectation of privacy against law enforcement in that information.[54]

5. Lulling people into revealing information

There is no Fourth Amendment doctrine that is clearly analogous to lulling people into revealing information through the social/anthropomorphic features of robots. But what case law there is suggests that the Fourth Amendment would not protect us from what we reveal to deceptive or reassuring robots. One could analogize the idea of the deceptive robot to a "false friend": police do not need a warrant to get information from a confidential informant, or friend who decides to turn on a person.[55] More broadly speaking, the Supreme Court has upheld deceptive behavior by police, including consent to enter a residence when police commit fraud, or falsely claim to be there for a legitimate purpose.[56] But if robots are instead analogized to

48. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

49. United States v. Davis, 754 F.3d 1205, 1217 (11th Cir. 2014) (finding that in light of *Jones*, the Fourth Amendment required a warrant for cell site location information and the Stored Communications Act protections were inadequate). *See also In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 312 (3d Cir. 2010).

50. *See, e.g.*, United States v. Knotts, 460 U.S. 276, 285 (1983).

51. *But see In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 609 (5th Cir. 2013).

52. *Warshak*, 631 F.3d at 266.

53. *Id.* at 286.

54. "[T]he mere ability of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy." *Id.*

55. Hoffa v. United States, 385 U.S. 293, 302 (1966) (finding no Fourth Amendment violation where petitioner "was relying upon his misplaced confidence that Partin would not reveal his wrongdoing"); Lewis v. United States, 385 U.S. 206, 212 (1966). The Supreme Court has held that police also do not need a warrant to bug a confidential informant with the informant's permission. United States v. White, 401 U.S. 745, 749 (1971).

56. Lewis v. United States, 385 U.S. 206, 211 (1966) ("A government agent, in the same manner as a private person, may accept an invitation to do business and may enter upon the premises for the very

diaries, rather than independent actors, then barring third party doctrine and storage of the information elsewhere, there may be a reasonable expectation of privacy in what gets revealed to a reassuring robot-friend.[57] Which analogy courts choose—the false friend, or the diary—may be central to how deceptive robots are treated in the law enforcement context.[58]

B. Private Parties

The government will not be the only party interested in information gathered by household robots. And as evidenced by the above discussion of the third party doctrine, private parties may actually have more direct access to information gathered by household robots than law enforcement will. It will be valuable for behavioral advertising, for modifying or monitoring robot behavior, and for innovating to fill unmet needs.

This Section evaluates several questions involving privacy violations by private parties. Most of these overlap with the questions addressed above in the context of Fourth Amendment doctrine. And interestingly, the answers in the case of private parties may differ. Thus contemplating household robots reveals interesting inconsistencies in U.S. privacy law, where some doctrinal areas may be evolving out of pace with others.

This Section first addresses how the law might treat privacy violations by private actors through robots that enter where they are not invited. Then it addresses robots that exceed the scope of their permitted entry into a private space by recording information revealed in that private space. It addresses implied assumptions of privacy risks; and actual contractual agreements. Finally, this Section discusses how to address robots that lull people into revealing more information to third parties than they intended, and, briefly, the question of whether household robots' recording of information about their environments could constitute "speech" by private parties.

1. Entering where not invited

Just as with Fourth Amendment doctrine, in privacy law addressing private actors, trespass and privacy violations can be linked. The privacy tort of intrusion upon seclusion does not technically hinge on location, but does in practice suggest that there is a reasonable expectation of privacy in privileged solitary places such as the

---

purposes contemplated by the occupant."). *See also* United States v. Contreras-Ceballos, 999 F.2d 432, 435 (9th Cir. 1993) ("we have held that a law enforcement officer's use of a ruse to gain admittance does not implicate section 3109 because it entails no breaking"); Dickey v. United States, 332 F.2d 773, 777–78 (9th Cir. 1964); Leahy v. United States, 272 F.2d 487, 489 (9th Cir. 1959). *See also* Elizabeth E. Joh, *Bait, Mask, and Ruse: Technology and Police Deception*, 128 HARV. L. REV. F. 246 (Apr. 2015).

However, police may not lie about the existence of a search warrant, or lie about their true purpose once they identify themselves as government. *See* Bumper v. North Carolina, 391 U.S. 543 (1968); United States v. Bosse, 898 F.2d 113 (9th Cir. 1990); United States v. Tweel, 550 F.2d 297 (5th Cir. 1977) ("It is a well established rule that a consent search is unreasonable under the Fourth Amendment if the consent was induced by the deceit, trickery or misrepresentation of the Internal Revenue agent."). *But see* United States v. Briley, 726 F.2d 1301, 1305 (1984) (finding that cryptic statements about the nature of the investigation do not necessarily invalidate consent to search).

57. *See* Riley v. California, 134 S.Ct. 2473, 2479 (2014) (referring to a diary as a "highly personal item").

58. Richards & Smart, *supra* note 21.

home.[59] If a robot enters a room where it is not invited, acting as an agent of a private party, then it may commit the intrusion tort. Here, a household robot's emergent behavior may create interesting problems around finding liability for those private actors who produced or allegedly control the robot.

California has legislated against the use of new technologies to gain access to areas where information could not previously have been gathered without trespassing.[60] This approach reflects Justice Scalia's language in *Kyllo*, the thermal imaging case, where Justice Scalia noted that virtual entrance into the home by technology not in public use was a Fourth Amendment violation.[61] If a robot is given permission to enter part of the home, and exceeds the scope of that permission by entering a forbidden location either physically or technologically, it might be in violation of this law in California.

2. Recording where they are invited to be, but not to record

A more interesting question in the case of private actors is whether robots that are invited to be in a location, but not invited to record there, commit a privacy violation. The alternative is that their activity—unlike law enforcement activity—might be protected by the First Amendment. I discuss this prospect more below, in B(6).

Existing case law points in both directions. On the one hand, some courts have found that granting permission to someone to be in a location constitutes granting permission to record, or at least obviates an expectation of privacy.[62] Other courts, however, have distinguished between inviting somebody in or confiding in them, and allowing them to record that interaction.[63]

In one case, a court held that even though a victim of a car crash understood that a nurse would witness and remember conversations, the crash victim's privacy was violated when those conversations were recorded.[64] In another, reporters who entered a quack "doctor's" home office by pretending to be patients were found by the Ninth Circuit to have violated the quack's privacy, even though they were not technically trespassing.[65] On the other hand, the Seventh Circuit found that news reporters who recorded fraudulent behavior at an eye doctor's office by posing as patients did not violate an expectation of privacy.[66]

The illicitly recording robot may face divided case law. The deciding factor may be a distinction noted by the Seventh Circuit: unpermitted recording in the home poses a greater privacy risk that unpermitted recording in public.[67]

59. RESTATEMENT (SECOND) OF TORTS § 652(b) (1977).
60. CAL. CIV. CODE § 1708.8(b) (Supp. 2015).
61. Kyllo v. United States, 533 U.S. 27, 34 (2001).
62. *See, e.g.*, Desnick v. ABC, Inc., 44 F.3d 1345, 1353–54 (7th Cir. 1995).
63. *See, e.g.*, Dietemann v. Time Inc., 449 F.2d 245, 249 (9th Cir. 1971).
64. Shulman v. Group W Prod., Inc., 955 P.2d 469, 497 (Cal. 1998).
65. *Dietemann*., 449 F.2d at 246, 249. *See also* Food Lion v. ABC Inc., 194 F.3d 505, 510 (4th Cir. 2001) (discussing First Amendment limits and duty of loyalty, more than privacy.).
66. *Desnick*, 44 F.3d at 1654–55.
67. *Id.* at 1352.

3. Implied Assumption of Risk (or Implied Consent)

As in Fourth Amendment cases, courts in cases about private actors often find no expectation of privacy where people assume a considerable risk that their actions will not be private. For example, as discussed earlier, the couple embracing at a fair were found not to have an expectation of privacy because they had assumed a risk of discovery by appearing together in a crowded, public space.[68] However, a woman photographed with her skirt up at a funhouse ride was not found to have assumed the risk of this photograph occurring, even though it took place in public, likely because her exposed body fell into the category of sensitive information.[69]

Assessment of whether owning a household robot implies consent to having information recorded may once again hinge on whether courts treat information revealed in the home as sensitive, or break it into subcategories where some information is not sensitive and some (for example, sexual or bodily information) is.[70]

4. Actual (Contractual) Agreements/Privacy Policies

The most interesting area of privacy law governing private actors with respect to household robots—and the area revealed to be most different from Fourth Amendment case law—involves actual contracts or privacy policies. Remember that in the Fourth Amendment context courts have applied the third party doctrine to find that people usually do not have an expectation of privacy in information revealed to third parties, reasoning that in revealing information to third parties a person consents to its not being private any more.[71] But in the private actor context, courts sometimes find expectations of privacy even when a person has technically consented to sharing that information with others.[72]

Christine Jolls has noted that in some contexts, courts outright ignore written agreements in cases evaluating privacy violations. Courts look beyond consent, even when it is given by written agreement, to substantive privacy norms.[73] Similarly, the Federal Trade Commission (FTC) uses its Section 5 authority to enforce against private companies not only when they fail to uphold their own privacy policies, but also when a privacy policy is found to be inadequate, or "unfair."[74]

In other words, in the Fourth Amendment context, courts use actual or implied consent to explain away a privacy interest, where in the private actor context, they may consider substantive privacy norms to find a privacy violation even where consent has technically been granted. In fact, the FTC's privacy enforcement takes place

68. Gill v. Hearst Pub. Co., 253 P. 2d 441, 445 (Cal. 1953).

69. Daily Times Democrat v. Graham, 162 So.2d 474, 478 (Ala. 1964).

70. *See, e.g.*, Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, 56 (May 2014), https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (suggesting the development of a taxonomy of kinds of information that can be collected without consent, with consent, or never).

71. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

72. Christine Jolls, *Rationality and Consent in Privacy Law* 55 (Yale Law School, Working Paper Dec. 10, 2010), available at http://www.law.yale.edu/documents/pdf/Alumni_Affairs/Jolls_RationalityandConsentinPrivacyLaw_1-21-10.pdf.

73. *Id.*

74. Woodrow Hartzog & Daniel J. Solove, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

when there is a relationship between a consumer and a company; while to the Fourth Amendment, the existence of that relationship means there is a lower privacy interest, if any exists at all.

A company drafting privacy policies for household robots may thus wish to strongly consider whether the policy adequately encompasses both industry standards and general privacy norms. As a practical matter, robots may be particularly ill-equipped to fit with the current U.S. notice-and-choice privacy regime, when they lack capabilities for consumers to input privacy choices or are designed to calm consumers into accepting their activity. [75]

5. Lulling People into Revealing Information

The reassuring or lying robot may receive harsh treatment when the deception is driven by private actors. The treatment of deceptive private actors varies even more noticeably from the Fourth Amendment's permissive treatment of "false friends" and lying law enforcement officers. Remember, when reporters lied and said they were patients to gain access to a quack "doctor's" home office, they were found to violate his privacy.[76]

The FTC also enforces against deceptive actors, who lie to get private information.[77] The FTC also, fascinatingly, enforces against actors that use technological design to elicit information, or to falsely indicate that something is private when it is not.[78] This line of FTC enforcement against deceptive or unfair technological design appears directly applicable to the anthropomorphic design characteristics of robots. If a robot appears trustworthy where it is not, it may be deemed deceptive by the FTC.[79]

6. Is Recording Speech (and whose)?

A final but very important issue with respect to the use of robots by private actors involves a line of developing First Amendment doctrine. A number of appellate courts have recognized some version of a First Amendment "right to record,"

---

75. Woodrow Hartzog, *Unfair and Deceptive Robots*, 74 Maryland L. Rev. 785, 794 (forthcoming 2015)(Mar. 23, 2015 8:03 AM), http://www.werobot2015.org/wp-content/uploads/2015/04/Hartzog-Unfair-Deceptive-Robots.pdf ("social robots are designed to draw us in"). *See also* Scott R. Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent*, 93 TEX. L. REV. 85, 140–41 (2014) (explaining with respect to the Internet of Things that "[t]he basic mechanism of notice and choice—to display and seek agreement to a privacy policy—can therefore be awkward in this context because the devices in question do not facilitate consent.").

76. Dietemann v. Time Inc., 449 F.2d 245, 245 (9th Cir. 1971); *but see* Desnick v. ABC, Inc., 44 F.3d 1345, 1345 (7th Cir. 1995).

77. *E.g.*, Press Release, FTC, Website Operator Banned from the 'Revenge Porn' Business After FTC Charges He Unfairly Posted Nude Photos (Jan. 29, 2015) *available at* https://www.ftc.gov/news-events/press-releases/2015/01/website-operator-banned-revenge-porn-business-after-ftc-charges.

78. Hartzog & Solove, *supra* note 74, at 642. (describing a line of FTC decisions on unfair design, and pointing to In re Sony BMG Music Entm't, FTC File No. 062 3019, No. C-4195 (F.T.C. June 28, 2007) and 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)).

79. Hartzog, *supra* note 75, at 20 (asking in the context of evaluating FTC enforcement against robots whether it matters that robots are "specifically designed to extract personal information through social engineering").

often in the context of citizens using their cellular telephones to record police officers.[80] A private company in Utah has used this "right to record" to challenge Utah's law governing information-gathering by automated license plate readers.[81] Utah amended the law so that it now applies only to law enforcement, and not private actors.[82]

There is a real question of whether household robots—or really, the private parties that built them or correspond with them—have a First Amendment "right to record" in private spaces. Most interactions will be governed by voluntary privacy policies that can be enforced by the FTC. But in instances where states wish to create new privacy laws, they may have to keep the First Amendment in mind. Once again, however, the fact that this information is being revealed and recorded in the home may outweigh any interest in "newsworthy" information that might be revealed, under First Amendment newsgathering doctrine. In light of Supreme Court case law rejecting distinctions between high value and low value speech, however, this argument might face obstacles in courts.

There is a legitimate question of whether robots or the private parties that programmed them constitute "speakers" at all.[83] Here, again, emergent behavior makes for an interesting conversation. How directly involved in recording decisions do private actors have to be, to garner First Amendment protection? If a private actor decides to "record all," will that gain more or less protection than somebody who records only short selections of information, or somebody who gives a robot the ability to make its own decisions about what to record?

IV. CONCLUSION AND SUMMARY OF WHAT HOME ROBOTS REVEAL

In conclusion, household robots reveal a number of interesting tensions in U.S. privacy law. While the tensions exist now, even before the widespread introduction of the new technology, the use of robots in the privileged private space of the household may bring these tensions to a head. Household robots, in other words, may be a doctrinal privacy catalyst.

Doctrinally, household robots will require courts to further consider the relationship between privacy, permission, and trespass. Courts will have to decide whether granting permission to an entity to be in a place also grants them permission to record information about that space. Courts will have to reconsider whether information can be private against a larger audience, even if one agrees to share it with a much smaller audience. Courts will also, in the Fourth Amendment context, have to

---

80. *See* ACLU of Ill. v. Alvarez, 679 F.3d 583, 595 (7th Cir. 2012), *cert. denied*, 133 S. Ct. 651 (2012); Glik v. Cunniffe, 655 F.3d 78, 83 (1st Cir. 2011); Smith v. City of Cumming, 212 F.3d 1332, 1333 (11th Cir. 2000); Kelly v. Borough of Carlisle, 622 F.3d 248, 262 (3d Cir. 2010).

81. Cyrus Farivar, *Private Firms Argue First Amendment Right to Collect License Plate Data*, ARS TECHNICA (Feb. 14, 2014, 10:00 AM), http://arstechnica.com/tech-policy/2014/02/14/private-firms-argue-first-amendment-right-to-collect-license-plate-data/.

82. Tim Cushing, *License Plate Reader Company Sues Another State For 'Violating' Its First Amendment Right To Build A 1.8-Billion-Image Database*, TECH DIRT (June 16, 2014, 3:37am) https://www.techdirt.com/articles/20140613/09224127569/license-plate-reader-company-sues-another-state-violating-its-first-amendment-right-to-build-18-billion-image-database.shtml.

83. *See generally* Stuart M. Benjamin, *Algorithms and Speech*, 161 U. PA. L REV. 1445-1493 (2013); Oren Bracha, *The Folklore of Informationalism: The Case of Search Engine Speech*, 82 FORDHAM L. REV. 1629 (2014); James Grimmelmann, Speech Engines, 98 Minn. L. Rev. 868 (2014).

reconcile treatment of the home as deserving of the utmost privacy protection with the third party doctrine.

Considering household robots reveals two interesting substantive splits between the Fourth Amendment approach to privacy, and the approach we use to address private actors. First, the Fourth Amendment tends to take a broad view of consent as obviating a privacy interest, while law governing private actors can be more skeptical; it sometimes looks to substantive privacy norms, or even protects privacy interests precisely because information has been shared with third parties.[84] Second, Fourth Amendment doctrine is more permissive of lying to get information, while law governing private actors enforces against deception—including deception by technological design.

But perhaps what household robots most reveal is the continued need in the United States for a holistic approach to big data. Currently, U.S. privacy law is a patchwork of sectoral federal laws, in contrast with the EU's holistic approach to data privacy.[85] To address both privacy and fairness problems raised by data gathering and analysis, we may wish to use household robots as an inspiration for enacting data privacy laws, based on Fair Information Practices. Such governance could include rules on collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, accountability, and individual participation.[86]

The United States currently relies on standards set by private parties and enforceable by the FTC. But perhaps the advent of household robots will finally bring truly home the notion that data processing carries with it real privacy and unfairness risks. Otherwise, Bill Gates's hope of a robot in every home may go unrealized, and many robots may—after a few prominent privacy violations— be left at the front door.

---

84. Jolls, *supra* note 72, at 55.

85. Although there has been discussion of the two approaches converging more in practice than the framework would indicate. See, e.g., Kenneth Bamberger and Deirdre Mulligan, Privacy on the Books and on the Ground, 63 Stan. L. Rev. (2011) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1568385.

86. These are the principles advocated by the OECD in its 1980 Privacy Guidelines, which in turn were based on the HEW Code of Fair Information Practices. *See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2013), http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm; *see also* Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems (July 1973), *available at* http://epic.org/privacy/hew1973report/default.html.