Consumer Cloud Robotics and the Fair Information Practice Principles: Recognizing the Challenges and Opportunities Ahead

Andrew Proia,* Drew Simshaw & Kris Hauser*****

ABSTRACT

Rapid technological innovation has made commercially accessible consumer robotics a reality. At the same time, individuals and organizations are turning to "the cloud" for more convenient and cost effective data storage and management. It seemed only inevitable that these two technologies would merge to create cloud robotics, "a new approach to robotics that takes advantage of the Internet as a resource for massively parallel computation and sharing of vast data resources." By making robots lighter, cheaper, and more efficient, cloud robotics could be the catalyst for a mainstream consumer robotics marketplace. However, this new industry would join a host of modern consumer technologies that seem to have rapidly outpaced the legal and regulatory regimes

---

© 2015 Andrew Proia, Drew Simshaw & Kris Hauser

* 2013–2014 Information Security Law & Policy Fellow, Indiana University Center for Applied Cybersecurity Research, J.D., Indiana University Maurer School of Law, 2013, B.S. in Criminal Justice, University of Central Florida, 2010. A working draft of this Article was presented at the We Robot 2014 Conference and benefited from the thoughtful comments by the Conference's attendees. The authors would like to also thank Professor Fred H. Cate for his thoughtful comments, as well as Dr. David Crandall and Dr. Selma Šabanović for their invaluable insight and contributions to numerous roundtable discussions that formed the basis of this Article.

** Policy Analyst, Indiana University Center for Law, Ethics, and Applied Research in Health Information, J.D., Indiana University Maurer School of Law, 2012, B.A. in Political Science, University of Washington, 2007.

*** Associate Professor, Duke University Pratt School of Engineering, Ph.D. in Computer Science, Stanford University, 2008, B.A. in Computer Science & B.A. in Mathematics, University of California at Berkeley, 2003.

implemented to protect consumers. Recently, consumer advocates and the tech industry have focused their attention on information privacy and security, and how to establish sufficient safeguards for the collection, retention, and dissemination of personal information while still allowing technologies to flourish. Underlying a majority of these proposals are a set of principles that address how personal information should be collected, used, retained, managed, and deleted, known as the Fair Information Practice Principles (FIPPs). This Article examines recent frameworks that articulate how to apply the FIPPs in a consumer setting, and dissects how these frameworks may affect the emergence of cloud-enabled domestic robots. By considering practical observations of how cloud robotics may emerge in a consumer marketplace regulated by the FIPPs, this research will help both the information privacy and robotics fields in beginning to address privacy and security challenges from a law and policy perspective, while also fostering collaboration between roboticists and privacy professionals alike.

INTRODUCTION

At the 2011 Google I/O Conference, Google's Ryan Hickman and Damon Kohler, and Willow Garage's Ken Conley and Brian Gerkey, took the stage to give a rather intriguing presentation: *Cloud Robotics, ROS for Java and Android*.[1] After giving a high-five to "PR2," a two-armed mobile manipulator robot built by Willow Garage,[2] Hickman demonstrated how robots like PR2, while amazing, are typically limited to on-board data storage and processing, which have limited capabilities due to weight and power constraints.[3] However, if robots were able to "tap into the cloud," as Hickman explained, the robot's data storage and processing could be "moved" into a remote server farm, which would take over the role of performing compute-intensive operations, such as those involved in 3D perception and navigation planning.[4] What Hickman demonstrated during the group's presentation is a concept known as "cloud robotics," a term accredited to Google Research Scientist Dr. James Kuffner that describes "a new approach to robotics that takes advantage of the Internet as a resource for massively parallel computation and real-time sharing of vast data resources."[5]

While the term "cloud robotics" is relatively new, the idea of using remote computational resources to drive robots has existed for over a decade.[6] In recent years, however, cloud computing infrastructure has greatly matured to the point where cloud storage providers,[7] computation providers,[8] and

---

1. Google Developers, *Google I/O 2011: Cloud Robotics*, YOUTUBE (May 11, 2011), http://www.youtube.com/watch?v=FxXBUp-4800.

2. *Id.*; *see also PR2: Overview*, WILLOW GARAGE, http://www.willowgarage.com/pages/pr2/overview (last visited Nov. 8, 2014); *Software: Overview*, WILLOW GARAGE, http://www.willowgarage.com/pages/software/overview (last visited Nov. 8, 2014).

3. Google Developers, *supra* note 1.

4. *Id*.

5. KEN GOLDBERG & BEN KEHOE, CLOUD ROBOTICS AND AUTOMATION: A SURVEY OF RELATED WORK 1 (2013), *available at* http://www.eecs.berkeley.edu/Pubs/TechRpts/2013/EECS-2013-5.pdf.

6. *See generally* Masayuki Inaba et al., *A Platform for Robotics Research Based on the Remote-Brained Robot Approach*, 19 INT'L J. ROBOTICS RES. 933, 933–39 (2000) (proposing a framework for "the remote-brained robot approach").

7. *See, e.g.*, *About Dropbox*, DROPBOX, https://www.dropbox.com/about (last visited Nov. 8, 2014); *Google Drive*, GOOGLE, https://www.google

computational paradigms[9] are now commonplace. Similar infrastructure advances for cloud-enabled robots are beginning to take shape. With experts estimating that personal and domestic robot sales will reach over 15 million units, at a value of over $5 billion between 2013 and 2016,[10] an innovation like cloud robotics could be a catalyst for the emergence of a mainstream consumer robot marketplace.

Cloud robotics as an industry, however, is very much in its infancy and still faces a number of challenges before it may be equated with mainstream tech devices like smartphones, tablets, and computers. As the creators of RoboEarth, a popular cloud robot architecture, have suggested, many legal,[11] moral,[12] safety,[13] and technical[14] questions must be resolved before the

---

.com/drive/ (last visited Nov. 8, 2014); *iCloud*, APPLE, https://www.apple.com/icloud/ (last visited Nov. 8, 2014).

8. *See, e.g.*, *Amazon EC2*, AMAZON, https://aws.amazon.com/ec2/ (last visited Nov. 8, 2014) (detailing the Amazon Elastic Compute Cloud web service); *Microsoft Azure*, MICROSOFT, http://azure.microsoft.com/en-us/ (last visited Jan. 3, 2014).

9. *See, e.g.*, Jeffrey Dean & Sanjay Ghemawat, *MapReduce: Simplified Data Processing on Large Clusters* 137 (USENIX 6th Symposium on Operating Sys. Design & Implementation, 2004) (detailing Google's MapReduce programming model); *What Is Apache Hadoop?*, HADOOP, http://hadoop.apache.org/ (last visited Nov. 8, 2014) (detailing the open source Apache Hadoop framework).

10. *See* INT'L FED'N OF ROBOTICS, EXECUTIVE SUMMARY, 2013 WORLD ROBOTICS: SERVICE ROBOTS 18–19 (2013), *available at* http://www.worldrobotics.org/uploads/tx_zeifr/Executive_Summary_WR_2013_01.pdf.

11. *See* Markus Waibel et al., *A World Wide Web for Robots—RoboEarth*, ROBOTICS & AUTOMATION MAG., June 2011, at 69, 79 (citing M. Ryan Calo, *Open Robotics*, 70 MD. L. REV. 571 (2011)).

12. *See* Waibel et al., *supra* note 11 (citing M. Ryan Calo, *Robots and Privacy*, *in* ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS 187–98 (Patrick Lin et al. eds., 2012) [hereinafter *Robots and Privacy*]).

13. *See* Waibel et al., *supra* note 11 (citing Koji Ikuta et al., *Safety Evaluation Method of Design and Control for Human-Care Robots*, 22 INT'L J. ROBOTICS RES. 281 (2003) (proposing a general method to evaluate safety of human care robots)).

14. *See* D. Lorencik & P. Sincak, *Cloud Robotics: Current Trends and Possible Use As a Service* 85 (IEEE 11th Int'l Symposium on Applied Machine Intelligence & Informatics, 2013) ("The main negative of using the cloud-based architecture is the possibility of losing the connection, and in this case, if robot uses the cloud services even for basic functionality, it will fail to do anything.").

practice of operating in unstructured environments and sharing data among robots becomes integrated into our everyday lives. One open question in particular is what effect cloud-enabled consumer robotics, particularly domestic service robots, will have on consumer privacy.[15]

Privacy advocates, policymakers, and government regulators have taken a keen interest in protecting the privacy of consumer data now that the Internet has become "integral to economic and social life in the United States," and as "[a]n abundance of data, inexpensive processing power, and increasingly sophisticated analytical techniques drive innovation in our increasingly networked society."[16] A number of recent attempts to provide meaningful and standardized consumer privacy protections have produced "privacy frameworks" intended to balance technological innovation with reasonable data collection, use, and retention limits.[17] Underlying the majority of these frameworks are a set of principles, first articulated in the 1970s, that address how personal information should be collected, used, retained, managed, and deleted, known as the Fair Information Practice Principles (FIPPs).[18] The FIPPs have been adopted in various forms, both nationally and internationally, as the foundational framework for both public and private sector entities to protect the privacy and integrity of personally identifiable information.[19] However, with cloud robotics sure to create a world in which independent machines "pool," "share," and "reuse" data, the integration of interconnected robots could

---

15. This Article borrows the definition of a "domestic service robot" as a robot "designed and priced for use within a home or other domestic environment." Tamara Denning et al., *A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons*, 105–06 (UBICOMP 11th Int'l Conf. on Ubiquitous Computing, 2009).

16. THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 5 (2012) [hereinafter WHITE HOUSE PRIVACY REPORT].

17. *E.g.*, FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS v–vi (2012) [hereinafter 2012 FTC PRIVACY REPORT].

18. *E.g.*, Robert Gellman, *Fair Information Practices: A Basic History*, BOB GELLMAN 1, http://bobgellman.com/rg-docs/rg-FIPShistory.pdf (last updated Aug. 3, 2014).

19. *Id.* at 6–9.

pose numerous challenges to FIPPs-based framework compliance.[20]

The privacy implications of robotics have been addressed from both legal and technical perspectives.[21] However, there is a lack of understanding about how current consumer privacy standards and proposed frameworks could affect the future of robotics as it integrates with the cloud and moves into our homes.[22] In particular, what practical challenges will cloud robotics face if it becomes a mainstream consumer industry and attempts to comply with the FIPPs? Should the cloud robotics industry begin to understand these challenges now, and if so, why? How can roboticists open a dialog with privacy advocates, policymakers, and regulators on how best to maintain both innovation and consumer privacy expectations as robots begin to connect to the Internet? These questions form the basis of this Article.

Section I introduces the concept of cloud robotics. This Section examines how, historically, robots have been limited by

---

20. *See, e.g.*, Waibel et al., *supra* note 11, at 70–71 (discussing pooled, shared, and reused data). *See generally* GOLDBERG & KEHOE, *supra* note 5 ("No robot is an island.").

21. *See, e.g.*, *Robots and Privacy*, *supra* note 12, at 187–98 (outlining "the effects of robots on privacy in[] three categories—direct surveillance, increased access, and social meaning . . . ."); Denning et al., *supra* note 15, at 105 (analyzing three household robots for security and privacy vulnerabilities, "identify[ing] key lessons and challenges for securing future household robots," and proposing "a set of design questions aimed at facilitating the future development of household robots that are secure and preserve their users' privacy"); Ryan Calo, *They're Watching. How Can That Be A Good Thing?*, STAN. MAG., Jan.–Feb. 2014, at 2–3 (suggesting that robots will "focus us in on the effects of living among sophisticated surveillance technologies" and open a "policy window" in which to update privacy law and policy).

22. *See* Denning et al., *supra* note 15, at 105 ("[T]here is currently a marked void in the consideration of the security and privacy risks associated with household robotics."). *But see* Aneta Podsiadła, *What Robotics Can Learn from the Contemporary Problems of Information Technology Sector: Privacy by Design as a Product Safety Standard—Compliance and Enforcement*, *in* WE ROBOT: GETTING DOWN TO BUSINESS 1, 1–3 (Stanford Univ. ed., 2013), *available at* http://conferences.law.stanford.edu/werobot/wp-content/uploads/sites/29/2013/04/What-robotics-can-learn-from-the-contemporary-problems-of-Information-Technology-sector.-Privacy-by-Design-as-a-product-safety-standard-compliance-and-enforcement.pdf (advocating for the adoption of "Privacy by Design" and "Security by Design" concepts to help minimize the privacy and security risks of domestic robots and proposing possible liability for robot manufacturers who fail to implement such concepts).

on-board, local processing and how cloud robotics, conversely, proposes a method to allow robots to "share knowledge and learn from each other's experiences" in order to "perform complex and useful tasks in the unstructured world in which humans actually live."[23] Section II provides a brief history of the FIPPs, with particular attention paid to their application in frameworks developed by the Federal Trade Commission (FTC) and the Obama Administration. Section III examines the unique FIPPs challenges facing cloud robotics within a domestic environment, such as a user's home. Finally, Section IV highlights the importance of considering these challenges today, and proposes possible next steps for both the information privacy and robotics communities.

I. CLOUD ROBOTICS AND TOMORROW'S DOMESTIC ROBOTS

The concept of "robots" is hard to clearly define, but robots are commonly considered to be multi-function devices with the capability to sense the current environment and act on that environment using movement.[24] Currently, robots can be found in a wide array of domains, from manufacturing, service, and medical robots, to robots used for national defense and space exploration.[25] Service robots, particularly those operating in domestic settings, have been deployed to assist people in their

---

23. P.H., *Artificial Intelligence Networks: We, Robots*, ECONOMIST (Jan. 21, 2014, 1:55 PM), http://www.economist.com/blogs/babbage/2014/01/artificial-intelligence-networks.

24. *See, e.g.*, Denning et al., *supra* note 15, at 105 (defining "robot" for their study as "a cyber-physical system with sensors, actuators, and mobility"); Bill Gates, *A Robot in Every Home*, SCI. AM., Jan. 2007, at 58 ("Although a few of the domestic robots of tomorrow may resemble the anthropomorphic machines of science fiction, a greater number are likely to be mobile peripheral devices that perform specific household tasks."); Neil M. Richards & William D. Smart, How Should the Law Think About Robots? 5 (May 11, 2013) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2263363 (proposing the definition of "robot" to be "a constructed system that displays both physical and mental agency, but is not alive in the biological sense" and "is something manufactured that moves about the world, seems to make rational decisions about what to do, and is a machine").

25. CONG. ROBOTICS CAUCUS ADVISORY COMM., A ROADMAP FOR U.S. ROBOTICS: FROM INTERNET TO ROBOTICS 3–4 (2013), *available at* http://www.cra.org/ccc/files/docs/2013-Robotics-Roadmap (outlining "Area Specific Conclusions" on a number of domains utilizing robotics).

daily lives, and compensate for mental and physical limitations.[26] While experts predict that robots incorporating "full-scale, general autonomous functionality" are still ten to fifteen years away,[27] the impact that cloud capabilities can have on robot intelligence could help bring service robots to a state of general autonomy sooner.

"Intelligence" is the connection between sensing and acting, which can be implemented in many ways.[28] Simple forms of intelligence include a set of fixed computational rules, such as if-then statements, or mathematical formulas, such as linear feedback controllers.[29] However, the intelligence needed to perform tasks expected of humans in unstructured environments, such as the home, must be much more complex.[30] Intelligent robots in domestic environments require incorporating rich, diverse sources of knowledge including images, 3D maps, object identities and locations, movement patterns of human occupants, physics simulators, and previous experience interacting with the environment.[31] As a result, modern general-purpose domestic robots are implemented as very large software systems, composed of multiple modules running sophisticated algorithms, each of which require significant computational power.[32]

Cloud-enabled robots, on the other hand, can outsource these systems and components.[33] In cloud robotics, the software for implementing intelligent or autonomous behavior is partially or fully shifted to "the cloud"—remote computers

---

26. *Id.* at 63.

27. *Id.* at 64.

28. *See* DAVID KORTENKAMP ET AL., ARTIFICIAL INTELLIGENCE AND MOBILE ROBOTS: CASE STUDIES OF SUCCESSFUL ROBOT SYSTEMS 4, 8 (David Kortenkamp et al. eds., 1998).

29. *See* Rodney A. Brooks, *Intelligence Without Representation*, 47 ARTIFICIAL INTELLIGENCE 139, 139–59 (1991).

30. *See* CONG. ROBOTICS CAUCUS ADVISORY COMM., *supra* note 25, at 65–67 (discussing the need for expanded research and development in the service robotics industry).

31. *See id.* at 67–72.

32. *See, e.g.*, *Why ROS?,* ROS.ORG, http://www.ros.org/core-components/ (last visited Nov. 8, 2014) (identifying some of the core parts of the robot operating system, ROS).

33. *E.g.*, GOLDBERG & KEHOE, *supra* note 5, at 1.

communicating to the robot via the Internet.[34] This moves the locus of "intelligence" from onboard the robot to a remote service.[35] There are several advantages to such an architecture. First, robots could be made cheaper because costs are reduced by eliminating the need for powerful onboard computers.[36] Moreover, robots may be able to use cheaper sensor and actuator hardware because more powerful computing resources can sometimes compensate for the inaccuracies of the hardware.[37] Fewer onboard computers also means lower energy usage and prolonged battery life, alleviating one of the great practical limitations currently faced by consumer robots.[38]

Second, the cloud may provide improved functionality. Computationally complex tasks, such as object recognition and planning, can be solved by "brute force" in the cloud with many parallel computers.[39] Moreover, the cloud has easier access to common information from the web and from other robots, which could improve the performance of tasks like object recognition due to the use of extensive existing databases on the web—such as image hosting web services like Google Image Search and Flickr—or the prior experience of other robots.[40] By vastly improving access to data, cloud-enabled robots will be better equipped to recognize and interact with objects within their environments.[41] Robots may also need to "call for help"

---

34. *See id.*

35. *Id.*

36. Erico Guizzo, *Robots with Their Heads in the Clouds*, IEEE SPECTRUM (Feb. 28, 2011, 9:10 PM), http://spectrum.ieee.org/robotics/humanoids/robots-with-their-heads-in-the-clouds.

37. *But see id.* ("In particular, controlling a robot's motion—which relies heavily on sensors and feedback—won't benefit much from the cloud.").

38. *See* Daniel J. Challou et al., *Parallel Search Algorithms for Robot Motion Planning*, 2 PROC. IEEE INT'L CONF. ON ROBOTICS & AUTOMATION 46, 46–51 (1993).

39. *See* Patrizio Dazzi, *A Tool for Programming Embarrassingly Task Parallel Applications on CoW and NoW*, ARXIV.ORG 1–2 (June 24, 2013), http://arxiv.org/pdf/1306.5782v1.pdf (providing an overview of parallel computing and listing examples of how the cloud can be effectively and efficiently used in this context).

40. *E.g.*, Guizzo, *supra* note 36.

41. *Id.*

when in a jam, and human tele-operators may be able to help, similar to Amazon's Mechanical Turk service.[42]

Finally, it is easier for a service provider to debug and update software on the cloud than in the consumer's home.[43] Software updates, for example, can occur seamlessly because a cloud service can update a cloud-enabled robot without having to physically access it.[44] Likewise, human technicians can perform remote debugging without physical access to the robot.[45]

Current cloud-enabled robots tend to use the cloud only for certain functions, such as object recognition, or to store large 3D maps.[46] But it is not hard to imagine that in the near future, a robot's intelligence could be fully shifted to the cloud. The robot will then locally implement a "thin client" that transmits sensor data to the service and receives instructions from the service.[47] The thin client may also perform some limited processing, particularly for calculations that must be done at a high rate, such as maintaining a motor position, or responding quickly and safely to unexpected collisions.[48]

---

42. *Amazon Mechanical Turk (Beta)*, AMAZON, http://aws.amazon.com/mturk/ (last visited Nov. 9, 2014).

43. *What Is Cloud Robotics?*, ROBOEARTH, http://roboearth.org/cloud_robotics/ (last visited Nov. 4, 2014) ("In addition, it removes overheads for maintenance and updates, and reduces dependence on custom middleware.").

44. *Id*.

45. *Id*.

46. *See, e.g.*, Markus Waibel & Gajan Mohanarajah, *Mapping in the Cloud*, ROBOHUB (Dec. 23, 2013), www.robohub.org/mapping-in-the-cloud/ ("[W]e have set up an inexpensive, light weight robot so that it can perform full 3D mapping in real-time by offloading heavy computation to the RoboEarth Cloud Engine.").

47. A "thin client" system is one in which a computer or program relies on other computers or programs to accomplish a particular computation. *See, e.g.*, Morgan Quigley et al., *ROS: An Open-Source Robot Operating System*, *in* ICRA WORKSHOP ON OPEN SOURCE SOFTWARE (2009), *available at* http://www.willowgarage.com/sites/default/files/icraoss09-ROS.pdf (proposing a "'thin' ideology" for a cloud-based ROS system that "encourage[s] all driver and algorithm development to occur in standalone libraries that have no dependencies on ROS").

48. *See* Agam Shah, *Powerful Thin Clients May Be Alternatives to PCs*, PCWORLD (May 23, 2013, 11:45 AM), http://www.pcworld.com/article/2039659/powerful-thin-clients-may-be-alternative-to-pcs.html (describing new thin clients introduced by Dell and Hewlett-Packard as now having faster processing, in part due to computing on the cloud, versus local computation).

Current cloud-enabled robots perform some limited perceptual processing to avoid transmitting huge amounts of sensor data, such as multiple video streams, to the cloud, but in the future it is likely that these bandwidth limitations will become less restrictive.[49] In the fully cloud-enabled case, the cloud service will see everything the robot sees.

It is not difficult to see that, if developed properly, cloud robotics could have a profoundly positive impact on the lives of millions. For example, the Institute for Alternative Futures (IAF) envisions a world where such technology will be able to help recovery from storms like cyclones by the early 2020s with the "innovation of humanitarian cloud robots that use[] software developed by an online community to detect cholera and other water-borne diseases."[50] In addition, "[t]he integration of social media and crowd-sourcing [will help] direct cloud robots in carrying potable water over long distances to those most in need."[51] However, the group also warns that cyber security breaches of cloud-enabled robots, like "home-based Eldercare robots," could cause "public cyber security anxiety" leading to "stringent robotic manufacturing and licensing regulations."[52] By the late 2020s, the IAF predicts that cyber security concerns could "ultimately slow[] robotics from realizing its full potential for offering societal benefits."[53]

As cloud robotics concepts continue to advance, entities are beginning to recognize the potential benefits such an architecture could have for home or domestic service robots. RoboEarth, for instance, is a well-known cloud robotics infrastructure based in Europe "that allows any robot with a network connection to generate, share, and reuse data."[54] The goal of RoboEarth is "to use the Internet to create a giant open

---

49. *See, e.g.*, Waibel & Mohanarajah, *supra* note 46 (viewing bandwidth as "a key driver for cloud-based robot services" and demonstrating a robot performing "full 3D mapping in real-time").

50. Ben Sheppard & Trevor Thompson, *Cyber Security for Robots: Scenarios for 2030—Cyber-Enhanced Well-Being or Artificial Retardation?*, INST. ALTERNATIVE FUTURES 3 (Feb. 3, 2014), http://www.roboticsbusinessreview.com/pdfs/Cyber_Security_for_Robots_Scenarios_IAF_5_Feb_2014_%281%29.pdf.

51. *Id.*

52. *Id.*

53. *Id.*

54. Waibel et al., *supra* note 11, at 71.

source network database that can be accessed and continually updated by robots around the world," thus allowing robots to enter "unstructured environments" and operate in the real world.[55] RoboEarth hopes that its architecture will create a "World Wide Web for robots" that will allow robots to operate efficiently in environments such as homes and hospitals.[56] In early 2014, the RoboEarth Consortium announced their fourth demonstration of RoboEarth, which featured "four robots collaboratively working together to help patients in a hospital."[57] Google has set its sights on a robot marketplace as well, and in 2013, Google "acquired seven technology companies in an effort to create a new generation of robots."[58] Google has also helped the advancement of cloud robotics with its products, such as Google Glass, which researchers have used for object recognition to implement robot-grasping tasks.[59]

From a privacy perspective, cloud robotics reveals a number of noteworthy characteristics. First, given the complexity of enabling robots to operate in an unstructured environment, the "datafication" of a robot's environment will be expansive and necessary.[60] This collection will include the detailed mapping of buildings and rooms, as well as particular data on objects within that environment, including data that will help determine what the object is and where the object is located.[61] Second, due to this unstructured environment,

---

55. *See Motivation*, ROBOEARTH, http://roboearth.org/motivation (last visited Nov. 4, 2014).

56. *See* Waibel et. al., *supra* note 11, at 70–71.

57. Gajamohan Mohanarajah, *RoboEarth 4th Year Demonstration*, ROBOEARTH (Jan. 13, 2014), http://roboearth.org/roboearth-public-demo-mini-symposium/.

58. John Markoff, *Google Puts Money on Robots, Using the Man Behind Android*, N.Y. TIMES, Dec. 4, 2013, at A1.

59. Ben Kehoe et al., *Cloud-Based Robot Grasping with the Google Object Recognition Engine*, 2013 IEEE INT'L CONF. ON ROBOTICS & AUTOMATION 4263, 4263 (2013), *available at* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6631180.

60. "Datafication," coined by Viktor Mayer-Schönberger and Kenneth Cukier, is the act of transforming something into "a quantified format so it can be tabulated and analyzed." VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 76–78 (2013).

61. *See* Waibel & Mohanarajah, *supra* note 46 ("Performing mapping in the cloud not only allows the creation of maps but also the ability to

unforeseen obstacles may make the data necessary to complete a specific task unknown at the time in which the data was collected.[62] Finally, the goal of pooling, sharing, and reusing data as a method of allowing robots to react and respond to unstructured environments suggests that data will not be used for a single purpose, but will be part of a complex architecture that may entail repurposing data for other tasks and for other robots.[63] It is this widespread and almost instantaneous collection of data, appropriation of data for unanticipated purposes, and sharing of data across multiple robots that raises privacy concerns and necessitates careful consideration of privacy best practices.

II. THE BACKBONE OF CONSUMER PRIVACY REGULATIONS AND BEST PRACTICES: THE FAIR INFORMATION PRACTICE PRINCIPLES

A. A LOOK AT THE FAIR INFORMATION PRACTICE PRINCIPLES

The FIPPs have been described as the "Gold Standard" for protecting personal information.[64] Robert Gellman, a noted privacy and information policy consultant, has described the FIPPs as a "set of internationally recognized practices for addressing the privacy of information about individuals."[65] The

---

understand them: By bringing computation close to the knowledge required to make sense of all of a robot's sensor information, Cloud Robotics offers robots a very powerful way to understand the world around them.").

62. Hani Hagras & Tarek Sobh, *Intelligent Learning and Control of Autonomous Robotic Agents Operating in Unstructured Environments*, 145 INFO. SCI. 1, 2 (2002) ("[I]t is not possible to have exact and complete prior knowledge of [changing unstructured] environments: many details are usually unknown, the position of people and objects cannot be predicted a priori, passageways may be blocked, and so on.").

63. P.H., *supra* note 23 (reporting comments made by RoboEarth scientists that "the 'nuanced and complicated' nature of life" outside controlled environments "cannot be defined by a limited set of specifications," and "to perform complex and useful tasks in the unstructured world in which humans actually live, robots will need to share knowledge and learn from each other's experiences").

64. *See Fair Information Practice Principles (FIPPs) Privacy Course*, BERKELEY SECURITY, https://security.berkeley.edu/fipps (last visited Nov. 4, 2014) ("Although these principles are not laws, they form the backbone of privacy law and provide guidance in the collection, use and protection of personal information.").

65. Gellman, *supra* note 18.

Obama Administration has defined the FIPPs as "the widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy."[66] At their inception, the FIPPs "reflected a wide consensus about the need for broad standards to facilitate both individual privacy and the promise of information flows in an increasingly technology-dependent, global society."[67]

The FIPPs' origins are largely attributed to a 1973 report, *Records, Computers, and the Rights of Citizens*, issued by the Department of Health, Education, and Welfare's Advisory Committee on Automated Personal Data Systems.[68] While investigating advancements in record-keeping systems, the Advisory Committee found that "a person's privacy is poorly protected against arbitrary or abusive record-keeping practices."[69] In order to diminish such practices, the report called for the enactment of a federal "Code of Fair Information Practice[s]" that would result in the core cannons of the FIPPs.[70]

The FIPPs were articulated in their most influential form in 1980 by the Organization for Economic Co-operation and

---

66. THE WHITE HOUSE, NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE: ENHANCING ONLINE CHOICE, EFFICIENCY, SECURITY, AND PRIVACY 45 (2011).

67. Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY 341, 341 (Jane K. Winn ed., 2006).

68. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS ix–xxxv (1973). Gellman notes that, at the same time as the Health, Education, and Welfare Report, a "Committee on Privacy" in Great Britain proposed many of the same principles. Gellman, *supra* note 18, at 3–4. In addition, the 1977 report by the Privacy Protection Study Commission, *Protecting Privacy in an Information Society*, "may have contributed to the development of [the FIPPs] . . . ." *Id.* at 4.

69. DEP'T OF HEALTH, EDUC. & WELFARE, *supra* note 68, at xx.

70. These principles included the following: "There must be no personal data record-keeping systems whose very existence is secret"; "[t]here must be a way for an individual to find out what information about him is in a record and how it is used"; "[t]here must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent"; and, "[t]here must be a way for an individual to correct or amend a record of identifiable information about him." *Id.*

Development (OECD).[71] Finding at the time that there was a "danger that disparities in national legislations could hamper the free flow of personal data across frontiers" that "could cause serious disruption in important sectors of the economy,"[72] the OECD sought "to develop Guidelines which would help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data."[73] The result, the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, represented "a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it."[74] These principles, reaffirmed in 2013, include: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.[75]

The FIPPs have been employed in many "different formulations coming from different countries and different sources over the decades,"[76] with several structural

---

71. Both the White House Consumer Privacy Bill of Rights and the Federal Trade Commission Privacy Framework, discussed *infra* Part II, have cited the OECD guidelines as guiding the creation of these more contemporary frameworks. *See* Gellman, *supra* note 18, at 6–7.

72. ORG. FOR ECON. CO-OPERATION & DEV., OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), *available at* http://www.oecd.org/internet/ieconomy/oecdguidelineson theprotectionofprivacyandtransborderflowsofpersonaldata.htm.

73. *Id.*

74. *Id.*

75. *See* ORG. FOR ECON. CO-OPERATION & DEV., THE OECD PRIVACY FRAMEWORK 13–15 (2013). In addition to reaffirming the traditional principles, the 2013 revisions aimed "to assess the Guidelines in light of 'changing technologies, markets and user behaviour, and the growing importance of digital identities.'" *Id.* at 3. The new concepts introduced in the revised OECD Guidelines include "[n]ational privacy strategies," describing how "a multifaceted national strategy co-ordinated at the highest levels of government" is required for "the strategic importance of privacy today," "[p]rivacy management programmes," which "serve as the core operational mechanism through which organisations implement privacy protection," and "[d]ata security breach notification," a new provision that "covers both notice to an authority and notice to an individual affected by a security breach affecting personal data." *Id.* at 4.

76. Gellman, *supra* note 18, at 1. *But see* Cate, *supra* note 67, at 341 (arguing that the FIPPs integration into U.S. and European law has caused the FIPPs to be "reduced to narrow, legalistic principles").

commonalities existing among them: (1) a delineation of scope; (2) procedural principles; and (3) substantive principles. The delineation of scope determines when fair information practices should apply, typically triggered by the information being collected or used.[77] The procedural principles "address how personal information is collected and used by governing the methods by which data collectors and data providers interact," and "ensure that [individuals] have notice of, and consent to, an entity's information practices."[78] The substantive principles "impose substantive limitations on the collection and use of personal information, regardless of consumer consent, by requiring that only certain information be collected and that such information only be used in certain ways."[79] Overall, when many speak of "the FIPPs," the principles they typically have in mind are the eight principles articulated in the OECD guidelines.

With the advent of the Internet, the tremendous increase in the collection and use of consumer data, and the increasing ubiquity of devices capable of collecting and storing more data, regulators have recently focused on developing ways in which the FIPPs can meet the data privacy challenges posed by modern technologies. Unlike other international regulations, no omnibus U.S. law regulates the use or collection of personal consumer data.[80] Federal statutes in the United States have been enacted that regulate data privacy and security practices for only a small subset of industry sectors and for particular

---

77. Most FIPPs-centric frameworks and regulations provide a subjective scope, recommending that the FIPPs apply only when the information is "sensitive" or "personally identifiable." *See infra* Parts II.B.1–C.1. However, this is not always the case. *See* Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALIF. L. REV. 877, 888–89 (2014) (explaining different U.S. approaches to determining personally indefinable information, including the "specific-types" approach).

78. FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 48–49 n.28 (1998).

79. *Id.*

80. Mary J. Culnan & Robert J. Bies, *Consumer Privacy: Balancing Economic and Justice Considerations*, 59 J. SOCIAL ISSUES 323, 332 (2003) ("Currently the U.S. government has adopted a reactive approach to addressing consumer privacy. For example, Congress typically . . . focuses on developing a narrowly-targeted (sectoral in contrast to omnibus) solution.").

types of data.[81] To some, such a regulatory scheme has resulted in "uneven protection for personal information and unequal treatment, even for similarly situated industry players."[82] Recognizing the need for modernized and universal information privacy and security practices, federal policymakers have started crafting updated privacy best practices that are based largely on the FIPPs and which reflect current commercial norms.[83] These recent frameworks attempt to balance the FIPPs with more flexible practices for companies. Many policymakers herald these frameworks as effective in providing consumer privacy best practices in our data-dependent society, and have advocated for legislation that would require companies to implement these baseline practices.[84]

Two recent frameworks offer a foundation on which to examine how cloud robotics may be affected by current calls for consumer privacy protection: the White House's Consumer Privacy Bill of Rights in its report, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy*, and the FTC's Privacy Framework in its report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* ("FTC Report").[85] These frameworks do not establish new FIPPs, but instead attempt to embody the

---

81. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 255–56 (2011). The FTC, as well, has become more aggressive in utilizing its enforcement authority under Section 5 of the Federal Trade Commission Act to regulate companies who have engaged in unfair or deceptive data privacy and security practices. *See, e.g.*, Decision and Order, Facebook, Inc., F.T.C. No. 092 3184 (Aug. 10, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf (alleging unfair and deceptive privacy practices concerning Facebook's 2009 change to its privacy controls). *See generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

82. Bamberger & Mulligan, *supra* note 81, at 257.

83. *See* 2012 FTC PRIVACY REPORT, *supra* note 17, at i–ii.

84. *See id.* at 12–14 ("[T]he commission calls on Congress to consider enacting baseline privacy legislation that is technologically neutral and sufficiently flexible . . . ."); *see also* WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 1–3 ("The Administration will encourage stakeholders to implement the Consumer Privacy Bill of Rights through codes of conduct and will work with Congress to enact these rights through legislation.").

85. WHITE HOUSE PRIVACY REPORT, *supra* note 16; 2012 FTC PRIVACY REPORT, *supra* note 17.

original concepts, like the OECD guidelines, "with some updates and changes in emphasis."[86] For instance, as this Article demonstrates, these frameworks have adopted practices that focus on the "context of the transaction"[87] or the "sensitivity" of the data[88] as methods for providing more flexible practices for companies to determine what data can be collected, how it can be used, and how long it can be retained.

Because it is unlikely that cloud-enabled domestic robots will be subject to today's industry-specific privacy regulations,[89] privacy advocates and policymakers will likely look to the practices articulated in these frameworks to determine the adequacy of cloud robotics companies' data practices. Thus, examining the Consumer Privacy Bill of Rights and the FTC Framework can assist in articulating challenges and developing discussion.

B. THE CONSUMER PRIVACY BILL OF RIGHTS

In February 2012, the White House observed that, despite the fact that the current consumer data privacy framework was strong, it "lack[ed] two elements: a clear statement of basic privacy principles that apply to the commercial world, and a sustained commitment of all stakeholders to address consumer data privacy issues as they arise from advances in technologies and business models."[90] It is within this context that the Obama Administration issued its report establishing a new privacy framework, the Consumer Privacy Bill of Rights. The report describes the Consumer Privacy Bill of Rights as "a blueprint for privacy in the information age" that "give[s] consumers clear guidance on what they should expect from

86. 2012 FTC PRIVACY REPORT, *supra* note 17, at 23.

87. *See infra* Part II.B.4.

88. *See infra* Parts II.B.1–C.1.

89. Cloud-enabled robots may, however, enter into commercial industry sectors that are in fact governed under specific information privacy regulations, such as the healthcare industry. *See, e.g.*, HIPAA Privacy Rule, 45 C.F.R. pts. 160, 164 (2013) (governing the collection, use, and dissemination of "protected health information" by covered health entities). For the purposes of this Article, we assume that cloud-enabled domestic robots, and the companies that produce and maintain them, operate outside of these sector-specific regulations.

90. WHITE HOUSE PRIVACY REPORT, *supra* note 16, at i.

those who handle their personal information, and set[s] expectations for companies that use personal data."[91]

As the Administration explains, "[t]he Consumer Privacy Bill of Rights applies comprehensive, globally recognized Fair Information Practice Principles . . . to the interactive and highly interconnected environment in which we live and work today."[92] The Administration acknowledges that "[t]he Consumer Privacy Bill of Rights applies FIPPs to an environment in which processing of data about individuals is far more decentralized and pervasive than it was when FIPPs were initially developed."[93] To "carr[y] FIPPs forward," the Consumer Privacy Bill of Rights "affirms a set of consumer rights that inform consumers of what they should expect of companies that handle personal data," while at the same time "recogniz[ing] that consumers have certain responsibilities to protect their privacy as they engage in an increasingly networked society."[94] The Consumer Privacy Bill of Rights consists of seven principles: individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability.[95] When applicable, the baseline principle is outlined, followed by supplemental information detailing the principle.

1. Scope

"The Consumer Privacy Bill of Rights applies to commercial uses of personal data. This term refers to any data, including aggregations of data, which is linkable to a specific individual. Personal data may include data that is linked to a specific computer or other device."[96] The Administration elaborates that "[t]his definition provides the flexibility that is necessary to capture the many kinds of data about consumers that commercial entities collect, use, and disclose."[97]

---

91. *Id.* (introductory statement of President Barack Obama).
92. *Id.* at 1.
93. *Id.* at 9.
94. *Id.*
95. *Id.* at 10.
96. *Id.* ("For example, an identifier on a smartphone or family computer that is used to build a usage profile is personal data.").
97. *Id.*

2. Individual Control

> *Consumers have a right to exercise control over what personal data companies collect from them and how they use it.*[98]

This principle contains two "dimensions," one placing obligations on companies and another defining the responsibilities of consumers.[99] The first dimension of the principle says, "at the time of collection, companies should present choices about data sharing, collection, use, and disclosure that are appropriate for the scale, scope, and sensitivity of personal data in question."[100] Consumer-facing companies "should give [consumers] appropriate choices about what personal data the company collects, irrespective of whether the company uses the data itself or discloses it to third parties."[101] Further, the Administration "encourages consumer-facing companies to act as stewards of personal data that they and their business partners collect from consumers," and believes that they "should seek ways to recognize consumer choices through mechanisms that are simple, persistent, and scalable from the consumer's perspective."[102]

In addition, the individual control principle has a second dimension regarding consumer responsibility.[103] In cases such as online social networks, where "the use of personal data begins with individuals' decisions to choose privacy settings and to share personal data with others . . . consumers should evaluate their choices and take responsibility for the ones that they make."[104]

---

98. *Id.* at 47.
99. *Id.* at 11.
100. *Id.* For example, in cases where a company has access to Internet usage histories capable of building profiles that may contain sensitive health or financial data, "choice mechanisms that are simple and prominent and offer fine-grained control of personal data use and disclosure may be appropriate." *Id.* On the other hand, "services that do not collect information that is reasonably linkable to individuals may offer accordingly limited choices." *Id.*
101. *Id.*
102. *Id.*
103. *Id.* at 13.
104. *Id.*

Finally, individual control contains a "right to withdraw consent to use personal data that the company controls."[105] According to the Administration, "[c]ompanies should provide means of withdrawing consent that are on equal footing with ways they obtain consent."[106] For this right to apply, the consumer must have an ongoing relationship with the company because "the company must have a way to effect a withdrawal of consent to the extent the company has associated and retained data with an individual," and therefore, "data that a company cannot reasonably associate with an individual is not subject to the right to withdraw consent."[107] Further, "the obligation to respect a consumer's withdrawal of consent only extends to data that the company has under its control."[108]

3. Transparency

> *Consumers have a right to easily understandable and accessible information about privacy and security practices.*[109]

Under the transparency principle, "companies should provide clear descriptions of what personal data they collect, why they need the data, how they will use it, when they will delete the data or de-identify it from consumers, and whether and for what purposes they may share personal data with third parties."[110] These statements should be made "[a]t times and in places that are most useful to enabling consumers to gain a meaningful understanding of privacy risks and the ability to exercise Individual Control."[111] This means that the statements should be made "visible to consumers when they are most relevant to understanding privacy risks and easily accessible when called for."[112] The form of these notices should be "easy to

105. *Id.*
106. *Id.* at 13–14 ("For example, if consumers grant consent through a single action on their computers, they should be able to withdraw consent in a similar fashion.").
107. *Id.* at 14.
108. *Id.*
109. *Id.*
110. *Id.*
111. *Id.*
112. *Id.*

read on the devices that consumers actually use to access their services."[113] According to the Administration, "[p]ersonal data uses that are not consistent with the context of a company-to-consumer transaction or relationship deserve more prominent disclosure than uses that are integral to or commonly accepted in that context."[114]

4. Respect for Context

> *Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.*[115]

A cornerstone of the Consumer Privacy Bill of Rights, the respect for context principle holds that "[c]ompanies should limit their use and disclosure of personal data to those purposes that are consistent with both the relationship that they have with consumers and the context in which consumers originally disclosed the data, unless required by law to do otherwise."[116] This means that "[i]f companies will use or disclose personal data for other purposes," or "[i]f, subsequent to collection, companies decide to use or disclose personal data for purposes that are inconsistent with the context in which the data was disclosed," then companies should provide heightened measures of transparency and individual choice.[117]

The Administration explains that the respect for context principle "emphasizes the importance of the relationship between a consumer and a company at the time consumers

---

113. *Id*. at 15. In the case of mobile devices, for instance, companies should "strive to present mobile consumers with the most relevant information in a manner that takes into account mobile device characteristics, such as small display sizes and privacy risks that are specific to mobile devices." *Id.*

114. *Id*. at 14 (finding that distinguishing privacy notices along these lines "will better inform consumers of personal data uses that they have not anticipated," "will give privacy-conscious consumers easy access to information that is relevant to them," and "may also promote greater consistency in disclosures by companies in a given market and attract the attention of consumers who ordinarily would ignore privacy notices").

115. *Id.* at 15. Respect for context, in part, derives from the OECD Framework's purpose specification and use limitation principles. *Id*. at 16; ORG. FOR ECON. CO-OPERATION & DEV., *supra* note 72, at 14–15.

116. WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 15.

117. *Id.*

disclose data, [but] also recognizes that this relationship may change over time in ways not foreseeable at the time of collection."[118] In such cases, "companies must provide appropriate levels of transparency and individual choice—which may be more stringent than was necessary at the time of collection—before reusing personal data."[119] While such context-specific application provides flexibility for companies, it requires them to consider what consumers are likely to understand about the companies' practices, how the companies explain the roles of personal data in delivering their products and services, and the consumers' attitudes, understanding, and level of sophistication.[120] According to the Administration, "[c]ontext should help to determine which personal data uses are likely to raise the greatest consumer privacy concerns" and "[t]he company-to-consumer relationship should guide companies' decisions about which uses of personal data they will make most prominent in privacy notices."[121]

5. Security

> *Consumers have a right to secure and responsible handling of personal data.*[122]

Under the security principle, "[c]ompanies should assess the privacy and security risks associated with their personal data practices and maintain reasonable safeguards to control risks such as loss; unauthorized access, use, destruction, or modification; and improper disclosure."[123] The Administration elaborates that "[t]he security precautions that are appropriate for a given company will depend on its lines of business, the

---

118. *Id.* at 16.

119. *Id.*

120. *Id.* at 16–17. For example, if a mobile game application collects the device's unique identifier for the purposes of executing the game's "save" function, such a collection is consistent with the consumer's decision to use the application. If the company provides the unique identifier to third parties for online behavioral advertising, then the respect for context principle calls for the company to notify consumers and allow them to prevent the disclosure of personal data. *Id.* at 17.

121. *Id.* at 16.

122. *Id.* at 19.

123. *Id.*

kinds of personal data it collects, the likelihood of harm to consumers, and many other factors."[124]

6. Access and Accuracy

> *Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.*[125]

According to the access and accuracy principle, companies "should use reasonable measures to ensure they maintain accurate personal data" and "provide consumers with reasonable access to personal data that they collect or maintain about them, as well as the appropriate means and opportunity to correct inaccurate data or request its deletion or use limitation."[126] Further, in selecting the appropriate methods "to maintain [data] accuracy and to provide access, correction, deletion, or suppression capabilities to consumers, companies may also consider the scale, scope, and sensitivity of the personal data that they collect or maintain and the likelihood that its use may expose consumers to financial, physical, or other material harm."[127] These factors "help to determine what kinds of access and correction facilities may be reasonable in a given context."[128]

7. Focused Collection

> *Consumers have a right to reasonable limits on the personal data that companies collect and retain.*[129]

The focused collection principle further states, "[c]ompanies should collect only as much personal data as they need to accomplish purposes specified under the Respect for Context principle," and that they "should securely dispose of or

---

124. *Id.*
125. *Id.*
126. *Id.*
127. *Id.*
128. *Id.* at 20.
129. *Id.* at 21.

de-identify personal data once they no longer need it, unless they are under a legal obligation to do otherwise."[130] This requires companies to "engage in considered decisions about the kinds of data they need to collect to accomplish specific purposes."[131]

8. Accountability

> *Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.*[132]

Within the report, the accountability principle lays out the ways in which "[c]ompanies should be accountable to enforcement authorities and consumers."[133] The accountability principle "goes beyond external accountability to encompass practices through which companies prevent lapses in their privacy commitments or detect and remedy any lapses that may occur."[134] Among other things, this means that companies "should hold employees responsible for adhering to these principles" and should appropriately train them "to handle personal data consistently with these principles and regularly evaluate their performance in this regard."[135] The appropriate evaluation technique could be a full audit, conducted by the company or by an independent third party, or a more limited self-assessment, depending on the "size, complexity, and nature of a company's business, as well as the sensitivity of the data involved."[136]

---

130. *Id.*

131. *Id.* However, "as discussed under the Respect for Context principle, companies may find new uses for personal data after they collect it, provided they take appropriate measures of transparency and individual choice." *Id.*

132. *Id.*

133. *Id.* at 21–22.

134. *Id.* at 22.

135. *Id.* at 21.

136. *Id.* at 22.

C. THE 2012 FEDERAL TRADE COMMISSION PRIVACY FRAMEWORK

Over the past two decades, the FTC has been actively engaged in overseeing information privacy and security practices within the online consumer marketplace.[137] In late 2009, former FTC Chairman Jon Leibowitz declared that the country was at a "watershed movement in privacy," and that the time was ripe for the FTC to "take a broader look at privacy writ large."[138] Recognizing the "increase[ed] advances in technology" that allowed for "rapid data collection and sharing that is often invisible to consumers," the FTC sought to develop a framework that businesses could utilize to reduce the burden on consumers who want to protect their own privacy.[139] In 2012, following a series of roundtable discussions and a period of public comment after the release of a preliminary report, the FTC issued *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* ("FTC Report").[140] The FTC Report was "intended to articulate best practices for companies that collect and use consumer data,"[141] and to assist companies in developing and maintaining "processes and systems to operationalize privacy and data security practices within their business."[142]

Central to the FTC Report is the FTC Framework, consisting of principles for companies to implement in order to

---

137. *See* FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS i–iv (2000) (summarizing the FTC's investigation of online privacy issues dating back to 1995).

138. Jon Leibowitz, Former Chairman, Fed. Trade Comm'n, Introductory Remarks at the FTC Privacy Roundtable (Dec. 7, 2009), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/introductory-remarks-ftc-privacy-roundtable/091207privacyremarks.pdf (citing to Samuel D. Warren and Louis D. Brandeis' publication, *The Right to Privacy*, in the Harvard Law Review, 4 HARV. L. REV. 193 (1890), and the surveillance abuses of the Nixon Administration as previous watershed moments in privacy).

139. Press Release, Fed. Trade Comm'n, FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers (Dec. 1, 2010) (on file with the FTC press release archive), *available at* http://www.ftc.gov/news-events/press-releases/2010/12/ftc-staff-issues-privacy-report-offers-framework-consumers.

140. 2012 FTC PRIVACY REPORT, *supra* note 17.

141. *Id.* at vii.

142. *Id.* at iii.

achieve best consumer privacy practices.[143] The FTC Report supplements the FTC Framework by providing in-depth commentary on the FTC Framework's final and baseline principles and suggesting practical mechanisms to implement the FTC Framework.[144] The FTC Framework's best practices are outlined in three areas—privacy by design, simplified consumer choice, and transparency—each of which delineates a "baseline principle," followed by a set of "final principles" that guide companies on protecting consumer privacy.[145]

1. Scope

According to the FTC Report, "[t]he framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device, unless the entity collects only non-sensitive data from fewer than 5,000 consumers per year and does not share the data with third parties."[146] The scope in which the FTC Framework applies is intentionally broad and intends to cover all entities collecting consumer data that can be reasonably linked to a specific consumer's computer or device, whether the information is online or offline.[147] Critical to the FTC Framework's scope is the requirement that consumer data be "reasonably linked to a specific consumer, computer, or other device."[148] The FTC Framework articulates that information will not be considered "reasonably linked" if three criteria are met: "[f]irst, the company must take reasonable measures to ensure that the data is de-identified"; "[s]econd, a company must publicly commit to maintain and use the data in a de-identified fashion, and not to attempt to re-identify the data"; and "[t]hird, if a company makes such de-identified data available to other companies—whether service providers or

143. *Id.* at vii–ix.

144. *See id*. at iii–vi (outlining the FTC's final report).

145. *Id.* at vii–viii.

146. *Id.* at 22.

147. *See id*. at 17–18. The FTC Privacy Report does note that some commercial sectors have statutory obligations already imposed upon them concerning proper data practices and that "the framework is meant to encourage best practices and is not intended to conflict with requirements of existing laws and regulations." *Id.* at 16.

148. *Id.* at 22.

other third parties—it should contractually prohibit such entities from attempting to re-identify the data."[149]

Additionally, the FTC Framework provides an exception for companies that collect non-sensitive data, for less than 5,000 consumers per year, and do not share that data with a third party.[150] The FTC Framework refrains from providing a set definition of what constitutes "sensitive" data, stating "whether a particular piece of data is sensitive may lie in the 'eye of the beholder' and may depend upon a number of subjective considerations."[151] However, the FTC Report does find that at a minimum, sensitive data includes "data about children, financial and health information, Social Security numbers, and certain geolocation data."[152]

2. Privacy by Design

> *Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.*[153]

The first major baseline principle under the FTC Framework is "Privacy by Design."[154] The concept of privacy by design calls on companies to "build in" substantive privacy principles and procedural protections into everyday business operations.[155] The privacy by design procedural principle states, "[c]ompanies should maintain comprehensive data management procedures throughout the life cycle of their products and services."[156] The FTC Report suggests that this principle can be achieved by implementing practices such as

149. *Id.* at 19–21. The FTC further specifies the first criterion, stating that it requires a company to "achieve a reasonable level of justified confidence that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device." *Id.* (citations omitted).

150. *Id.* at 22.

151. *Id.* at 60.

152. *Id.* at 47 n.214.

153. *Id.* at 22.

154. *Id*.

155. *Id.*

156. *Id.* at 32.

accountability mechanisms to ensure that privacy issues are addressed throughout an organization and its products.[157]

These mechanisms are intended to ensure the proper implementation of the privacy by design substantive principles specifically, and the FTC Framework generally.[158] The privacy by design procedural principle, thus, accompanies a substantive principle that articulates what data management procedures should be implemented. The privacy by design substantive principle states, "[c]ompanies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention practices, and data accuracy."[159]

As the FTC Report notes, "[i]t is well settled that companies must provide reasonable security for consumer data."[160] While no specific security practices are detailed, the FTC Report "calls on industry to develop and implement best data security practices for additional industry sectors and other types of consumer data."[161]

In calling for "reasonable" collection limits, the FTC Report clarifies that "[c]ompanies should limit data collection to that which is consistent with the context of a particular transaction or the consumer's relationship with the business, or as required or specifically authorized by law."[162] Data collection that is inconsistent with the context of a particular transaction should be appropriately disclosed to consumers "at a relevant time and in a prominent manner—outside of a privacy policy or other legal document."[163] Similar to the White House Consumer Privacy Bill of Rights Framework discussed above,[164] limiting data collection to the context of the transaction "is intended to help companies assess whether their data collection is consistent with what a consumer might expect."[165]

---

157. *Id.* at 30–32.
158. *Id.*
159. *Id.* at 23.
160. *Id.* at 24.
161. *Id.* at 25.
162. *Id.* at 27.
163. *Id.* For a more in-depth discussion on consumer choice, see *infra* Part II.C.3.
164. *See supra* Part II.B.7.
165. 2012 FTC PRIVACY REPORT, *supra* note 17, at 27.

While collection limits focus on the amount of data a company collects, "sound data retention" practices focus on the length of time for which collected data should be retained.[166] The FTC Report states, "companies should implement reasonable restrictions on the retention of data and should dispose of it once the data has outlived the legitimate purpose for which it was collected."[167] A reasonable period under the FTC Framework "can be flexible and scaled according to the type of relationship and use of the data."[168] Regardless of the determined reasonable retention period, the FTC Report states that companies should ensure that their retention period standards are clear and properly followed by employees.[169]

Finally, companies should "take reasonable steps to ensure the accuracy of the data they collect and maintain, particularly if such data could cause significant harm or be used to deny consumers services."[170] However, recognizing the need to create flexibility for companies, the FTC Report notes "the best approach to improving the accuracy of the consumer data companies collect and maintain is a flexible one, scaled to the intended use and sensitivity of the information."[171]

3. Simplified Consumer Choice

Companies should simplify consumer choice.[172]

Due to "the dramatic increase in the breadth of consumer data," the lack of legal requirements on companies to provide consumer choices, and the inadequacy of privacy policies to effectively communicate consumer choices, the simplified consumer choice principle recommends methods of choice that

166. *Id.* at 27–29.
167. *Id.* at 28.
168. *Id.*
169. *Id.* at 29.
170. *Id.* (referencing the 2010 preliminary staff report which preceded the final 2012 report).
171. *Id.* ("[C]ompanies using data for marketing purposes need not take special measures to ensure the accuracy of the information they maintain. Companies using data to make decisions about consumers' eligibility for benefits should take much more robust measures to ensure accuracy . . . .").
172. *Id.* at 35.

are intended to be more effective and less burdensome on consumers.[173] The simplified consumer choice principle is broken down into two parts: when consumer choice may be unnecessary,[174] and what constitutes an appropriate method of consumer choice when such choice is necessary.[175]

First, "[c]ompanies do not need to provide choice before collecting and using consumer data for practices that are consistent with the context of the transaction or the company's relationship with the consumer, or are required or specifically authorized by law."[176] Similar to the Consumer Privacy Bill of Rights, the FTC Framework states that the "context of the transaction" standard generally depends on reasonable consumer expectations but "focuses on more objective factors related to the consumer's relationship with a business."[177] The FTC Report expands on its discussion of the context standard, explaining how product or service "fulfillment, fraud prevention, internal operations, legal compliance and public purpose, and most first-party marketing . . . provide illustrative guidance regarding the types of practices that would meet the . . . standard and thus would not typically require consumer choice."[178]

Second, in the event that choice would be appropriate, the FTC Framework's simplified consumer choice principle states:

> [C]ompanies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data. Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes.[179]

---

173. *Id.*

174. *Id.* at 36–48.

175. *Id.* at 48–60.

176. *Id.* at 48.

177. *Id.* at 38 ("[F]or some practices, the benefits of providing choice are reduced—either because consent can be inferred or because public policy makes choice unnecessary.").

178. *Id.* at 38–39 (citations omitted). The FTC Report does expand, however, on certain practices in which consumer choice would be appropriate, such as tracking across other parties' websites, *id.* at 40–41, third-party marketing, *id.* at 41–42, collection of sensitive data for first-party marketing, *id.* at 47–48, and for certain data enhancement practices, *id.* at 42–44.

179. *Id.* at 60.

In regard to when choice should be provided, the FTC Report clarifies that companies should "offer clear and concise choice mechanisms that are easy to use and are delivered at a time and in a context that is relevant to the consumer's decision about whether to allow the data collection or use."[180] Again, relying on the idea of context, the FTC Report does not define an ironclad point at which choices must be offered to a consumer, but instead calls on companies to account for the nature or context of the consumer's interaction with a company or the type or sensitivity of the data at issue.[181]

The method of choice also plays into the context determination. The FTC Report, for instance, explains that companies should not utilize "take-it-or-leave-it" choice mechanisms outside the context of the interaction between company and consumer.[182] At the same time, flexibility is needed in order to avoid "choice fatigue."[183] As the FTC Report states, "[c]onsumers' privacy interests ought not to be put at risk in . . . one-sided transactions."[184] Overall, companies are tasked with providing consumers with choices at a time and in a context that is meaningful and relevant to the consumer.

In a number of circumstances, the FTC Report suggests that a heightened degree of consumer choice, referred to as "affirmative expressed consent,"[185] is appropriate when information is used "(1) . . . in a materially different manner than claimed when the data was collected; or (2) [when] collecting sensitive data for certain purposes."[186] The FTC Report explains that use of consumer data in a "materially different manner" may be determined on a "case-by-case basis."[187] The FTC Report also states that affirmative

---

180. *Id.* at 49–50.

181. *Id.* at 50.

182. *Id.* at 51–52. "Take-it-or-leave-it" or "walk away" choice mechanisms are methods that "make a consumer's use of its product or service contingent upon the consumer's acceptance of the company's data practices." *Id.* at 50.

183. *Id.* at 49.

184. *Id.* at 52.

185. *Id.* at 57 n.274 ("Companies may seek 'affirmative express consent' from consumers by presenting them with a clear and prominent disclosure, followed by the ability to opt in to the practice being described.").

186. *Id.* at 60.

187. *Id* at 58. For example, "sharing consumer information with third parties after committing at the time of collection not to share the data." *Id.*

expressed consent should be obtained before collecting sensitive data.[188]

4. Transparency

> *Companies should increase the transparency of their data practices.*[189]

Specifically, the transparency principle includes a privacy notice final principle and an access final principle.[190] Under the privacy notice final principle, the FTC Framework states that "[p]rivacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices."[191] The FTC Report recommends that "privacy statements should contain some standardized elements, such as format and terminology, to allow consumers to compare the privacy practices of different companies and to encourage companies to compete on privacy."[192] However, the FTC Report notes that such standardization can be difficult when technologies vary in their hardware specifications, such as mobile devices with smaller screens.[193]

Under the access final principle, the FTC Framework states that "[c]ompanies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use."[194] The FTC Report specifies that some uses of consumer data, such as for "marketing purposes," may have costs associated with access mechanisms that outweigh the

188. *See id.* at 58–60.

189. *Id.* at 60.

190. *Id.* at 60–71. The FTC Framework's transparency principle also includes a third final principle, the consumer education principle, which states that "[a]ll stakeholders should expand their efforts to educate consumers about commercial data privacy practices." *Id.* at 72. Because this principle goes beyond the purposes of this Article, it is not discussed.

191. *Id.* at 64.

192. *Id.* at 62.

193. *See id.* at 63–64.

194. *Id.* at 71.

benefits.[195] Other uses of consumer data, such as decision-making purposes that fall outside of statutory requirements, would require more consumer access. Overall, the FTC Report states that the access final principle "supports the sliding scale approach . . . with the consumer's ability to access his or her own data scaled to the use and sensitivity of the data."[196]

III. WHEN THE FAIR INFORMATION PRACTICE PRINCIPLES MEET CLOUD ROBOTICS: PRIVACY IN A HOME OR DOMESTIC ENVIRONMENT

By using the above frameworks as a guide, we can begin to understand how the FIPPs may frame consumer privacy discussions regarding cloud-enabled domestic robots. Cloud robotics introduces distinct characteristics that differentiate it from other technologies at the center of current data privacy and security policy debates.[197] These distinctions will become critical when considering proper data collection and use practices.[198] By understanding these concepts, roboticists may be empowered to constructively contribute to the debate over how to properly regulate data in the up-and-coming consumer robot marketplace.[199] Technologists and roboticists alike can begin to research the development of privacy-enhancing technologies.[200] Throughout this evaluation, this Section recognizes some practical challenges cloud robotics may face in applying the FIPPs.[201] Where appropriate, similarities and distinctions from current technologies are presented, and possible alternative solutions are raised.

This Section begins by considering how to properly characterize data collected by a cloud-enabled domestic robot,

---

195. *Id.* at 65–66. ("The Commission does, however, encourage companies that maintain consumer data for marketing purposes to provide more individualized access when feasible.").

196. *Id.* at 67 ("At a minimum, these entities should offer consumers access to (1) the types of information the companies maintain about them; and (2) the sources of such information.") (internal footnotes omitted).

197. *See infra* notes 257–64 and accompanying text.

198. *See infra* Part III.B.

199. *See infra* notes 417–18 and accompanying text.

200. *See infra* notes 417–26 and accompanying text.

201. *See infra* Part III.A–G (highlighting these practical challenges in each section).

including the issue of whether to classify data related to objects found within a domestic environment as "sensitive."[202] Recognizing that, at the very least, information collected, used, and retained by cloud-enabled robots will likely be reasonably identifiable, this Section highlights the difficulty of determining which data practices will be considered "within the context" of a cloud-enabled domestic robot transaction, and what effect that might have on data collection, use, and retention limitations.[203] Next, this Section highlights the difficulties cloud robotics companies will face in determining how and when to properly disclose data practices to a user in order to present meaningful choice mechanisms.[204] Finally, the principles of transparency,[205] security,[206] access and accuracy,[207] and accountability[208] are explored.

This, like most attempts to explore the effects of robots on society, is very much a thought experiment and merely opens the door to the many privacy questions that will arise as cloud robotics begins to enter the consumer marketplace. In order to focus discussion, this Section limits the scope in which it examines cloud robotics. First, this Section focuses primarily on the privacy implications that arise directly between the consumer-facing cloud robotics company and the user.[209]

---

202. *See infra* Part III.A.
203. *See infra* Part III.B.
204. *See infra* Part III.C.
205. *See infra* Part III.D.
206. *See infra* Part III.E.
207. *See infra* Part III.F.
208. *See infra* Part III.G.
209. This focus is intended for a number of reasons. First, cloud robotics is in its infancy and thus limits the authors' ability to determine how the cloud robotics ecosystem will develop. Similar to the mobile environment, where smartphone hardware manufacturers, phone software operating system providers, and mobile application service providers may be separate and distinct entities, the cloud robotics ecosystem, too, could involve a host of companies at each of the hardware, software, and service levels. Limiting examination to interaction between a consumer-facing cloud robotics company and the users allows us to pay direct attention to the first-party privacy challenges that may arise. Second, because these first-party interactions are just beginning to be understood, addressing the more complex privacy issues arising from the collection, use, and retention of data from entities that neither directly interact with the consumer nor maintain the robot collecting a user's data—sometimes referred to as third-party entities—may be premature.

Second, this Section is limited to the privacy issues that might arise from cloud-enabled robots "designed and priced for use within a home or other domestic environment"[210]—which we refer to as cloud-enabled domestic robots—and the companies that will market, produce, and maintain them.

A. THE DATA AT ISSUE: LINKABLE DATA AND THE "SENSITIVITY" OF DATA COLLECTED BY CLOUD-ENABLED DOMESTIC ROBOTS

Before cloud-enabled robots enter the home, companies will need to fully understand whether the information their robots will collect is reasonably linked to a consumer or device, and the exact "sensitivity" of such data.[211] Generally speaking, the FIPPs apply to data that is "personally identifiable" to a person or device.[212] While it is likely that the information collected, stored, and retained by cloud-enabled domestic robots will be personally identifiable, the more challenging task will be determining data sensitivity.

1. Information Linked to a Consumer or Cloud Robot

The first question in any framework analysis is whether the information at issue is reasonably linkable to specific consumers, computers, or devices.[213] Information that can be reasonably linked to the consumer or cloud-robot, sometimes referred to as "personally identifiable information" (PII), will trigger the framework's application.[214] Thus, if the information

---

As cloud robotics continues to develop, it would be wise to consider the privacy implications that may arise from these additional issues.

210. Denning et al., *supra* note 15, at 106.

211. *See supra* notes 194–96 and accompanying text.

212. *See supra* Part II.B.1–C.1.

213. *See supra* Part II.B.1–C.1.

214. The question of how best to specifically define PII has spawned a large debate among privacy scholars. *See, e.g.*, Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1704–06 (2010) (arguing that the "squabbles over magical phrases like 'personally identifiable information' (PII) or 'personal data'" miss the point as advances in re-identification have made exploitation of non-PII possible and advocating for the search for a new approach to protecting privacy); Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1817 (2011) (arguing that the PII concept is important but "must be reconceptualized if privacy law is to remain effective in the future"). This Article does not attempt

collected by a cloud-enabled domestic robot cannot be reasonably linked to a consumer or the robot itself, or if the linkable information collected meets one of the exceptions delineated within the frameworks,[215] then no further practices would be required of that company's collection, use, or retention of that information.

Current concepts in cloud robotics make it likely that cloud-enabled domestic robots will rely on data reasonably linkable to the robot, and possibly even to the consumer.[216] For instance, the data RoboEarth collects, uses, and retains is identifiable in that it relies on maintaining geolocation metadata on the robot's environment and the objects within that environment.[217] The "Environment" table in RoboEarth's database will store detailed environment data, including the geographical coordinates of a particular environment, floor plans, and map data down to the particular room of a building.[218] Object data collected and stored contain precise tags that include the location of an object, as well as the time an object was detected.[219] Thus, the geolocation metadata tags captured, utilized, and stored by a cloud-enabled robot will likely mean that much of the data are linkable to the robot and possibly the user.[220]

Certain methods and practices, however, could be utilized in order to de-identify data, preventing application of the FIPPs in the first place.[221] The FTC Framework, for instance, would not consider data that companies take reasonable steps to "de-identify" as linked to a user or device, so long as the company

---

to solve the PII definitional problem, but acknowledges that the debate itself will be affected by the complexity of cloud robotics.

215. For instance, the FTC Framework will exempt an entity that: (1) collects nonsensitive data; (2) from fewer than 5000 consumers per year; and (3) does not share that data with third parties. 2012 FTC PRIVACY REPORT, *supra* note 17, at 22; *see supra* Part II.C.1.

216. *See* Waibel et al., *supra* note 11, at 75.

217. *See id*.

218. BJÖRN SCHIEßLE ET AL., COMPLETE SPECIFICATION OF THE ROBOEARTH PLATFORM 13 (2010), *available at* http://roboearth.org/wp-content/uploads/2011/03/D61_V2.pdf.

219. *See* Waibel et al., *supra* note 11, at 73–75 (explaining how objects, environments, and action recipes are stored).

220. *See generally id.* (explaining the various ways the robots are linked with the data).

221. *See infra* notes 222–24.

commits to not re-identifying the data.[222] Numerous privacy-enhancing technologies have been created to help reasonably de-identify data,[223] and other de-identification methods that would allow for cloud-enabled domestic robots to still function effectively in a home environment could greatly offset any burdens that other FIPPs principles might have on the commercialization of these robots. However, in practice, privacy enhancements may offset the functional advantages of keeping data personally identifiable.[224]

2. Sensitivity of Information Linked to a Consumer or Cloud Robot

A more challenging issue will be determining data sensitivity. The term "sensitive," as used by the recent frameworks, is intentionally subjective in order to provide flexibility. The FTC Framework, for instance, states that the determination is one that is "in the eye of the beholder."[225] However, the term is one of significant importance for companies attempting to adhere to the FIPPs, as the "sensitivity" of PII, in many cases, will influence the rigidity of the framework's practices.[226] Posing the question of what is "sensitive" data to a world where cloud-enabled robots are operating within the home raises numerous questions.

---

222. *See supra* Part II.C.1. In the case of third-party interactions, the entity must also agree to hold third parties to an agreement that they too will not re-identify the information. *Id.*

223. *See e.g.*, Robert Templeman et al., *PlaceAvoider: Steering First-Person Cameras Away from Sensitive Spaces* 1 (Network & Distributed Sys. Security Symposium, 2014) (demonstrating the "PlaceAvoider" technique for first-person cameras, which "'blacklist' sensitive spaces . . . [by] recogniz[ing] images captured in these spaces and flag[ing] them for review before the images are made available to applications").

224. *See* Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1200–01 (2012) ("Anonymous information derived from autonomous vehicles should be sufficient for such uses as transportation planning, traffic management and the like. The challenge will be to maintain the anonymity of this information, which often gains value when linked to an identifiable person.").

225. 2012 FTC PRIVACY REPORT, *supra* note 17, at 60.

226. *See, e.g.*, *supra* Part II.C.3 (explaining that the FTC Framework may require affirmative expressed consent from the user before collecting sensitive data); *see also supra* Part II.B.2 (recommending that consumer "choices about data sharing, collection, use, and disclosure . . . [should be] appropriate for the scale, scope, and *sensitivity* of personal data in question") (emphasis added).

Traditionally, "sensitive" information has been designated to certain classifications of data content.[227] For instance, the FTC Framework concluded from a "consensus" among comments made to the FTC while authoring their Framework that "information about children, financial and health information, Social Security numbers, and precise, geolocation data" are categories of sensitive information.[228] Others have argued that certain categories of content information, such as "race, religious beliefs, and criminal records," should be classified as "per se" sensitive.[229] Under this approach, the content of the information alone can dictate sensitivity, regardless of other facts such as where or how this information was collected.[230] Some difficulties emerge, however, when attempting to properly classify the content of information and trying to establish a consensus as to how sensitive the information may be.[231] Robots, particularly cloud-enabled domestic robotics, provide an opportunity to consider new content classifications of information that current technologies have not previously collected.[232]

However, the home environment itself brings unique challenges to determining levels of sensitivity, and may spawn discussions outside of the traditional content categorization approach as home technologies continue to advance. An individual's home, and the items within it, have traditionally

---

227. *See, e.g.*, *supra* note 152 and accompanying text.

228. 2012 FTC PRIVACY REPORT, *supra* note 17, at 58.

229. ORG. FOR ECON. CO-OPERATION & DEV., *supra* note 72, at 55 (explaining that some approaches to determining sensitivity, such as those reflected in European legislation, "enumerate types or categories of data which are per se sensitive and the collection of which should be restricted or even prohibited").

230. *See id.*

231. The OECD described this issue in its original explanatory memorandum to the OECD Privacy Guidelines. *Id.* at ch. 3. The memo explained that "[d]ifferent views are frequently put forward" with respect to determining which information is "specially sensitive" based upon "the manner in which they are to be processed, their nature, the context in which they are to be used or other circumstances." *Id.* at 55. In the end, "[t]he Expert Group discussed a number of sensitivity criteria . . . but has not found it possible to define any set of data which are universally regarded as sensitive." *Id.*

232. *See Robots and Privacy*, *supra* note 12, at 192–94 (describing how robots will provide new surveillance opportunities because they will be "inadvertently grant[ed] access to historically private spaces and activities").

been afforded heightened privacy protections. Constitutionally, we have seen an individual's "residential privacy" interest outweigh another's First Amendment right to freedom of speech.[233] Additionally, government entities are required to obtain a warrant for searches within an individual's home because of the heightened expectation of privacy the location provides, regardless of "the quality or quantity of information obtained."[234] In their report to President Obama entitled *Big Data and Privacy: A Technological Perspective*, the President's Council of Advisors on Science and Technology also recognized the privacy challenges the home's "special status" will create as "audio, video, and sensor data . . . [are increasingly] generated within the supposed sanctuary of the home."[235] In summary, any linkable information collected by cloud-enabled domestic robots could be considered sensitive simply because it is collected within the home, and would induce heightened privacy protections.

The FTC itself has suggested in a recent complaint that otherwise non-sensitive information, if collected within the home, could be considered "sensitive."[236] In late 2013, the FTC filed a complaint against TRENDnet, a tech company that sold Internet-enabled video cameras, for engaging in deceptive and unfair trade practices in violation of Section 5 of the Federal Trade Commission Act.[237] In its complaint, the FTC claimed that TRENDnet's lax security practices "subjected its users to a significant risk that their sensitive information, namely the

---

233. *See, e.g.*, Frisby v. Schultz, 487 U.S. 474, 486 (1988) (holding that targeted residential picketing "inherently and offensively intrudes on residential privacy" and that such activities can have a "devastating effect . . . on the quiet enjoyment of the home"); FCC v. Pacifica Found., 438 U.S. 726, 748 (1978) ("[T]he individual's right to be left alone plainly outweighs the First Amendment rights of an intruder.").

234. Kyllo v. United States, 533 U.S. 27, 37 (2001). In addition, the Supreme Court has said, "[a]t the Fourth Amendment's 'very core' stands 'the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'" Florida v. Jardines, 133 S. Ct. 1409, 1412 (2013) (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

235. PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 14–17 (2014).

236. Complaint, TRENDnet, Inc., F.T.C. No. 122 3090, at 4–6 (Sept. 4, 2014) [hereinafter TRENDnet], *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/09/130903trendnetcmpt.pdf.

237. *Id.* at 7.

live feeds from its IP cameras, will be subject to unauthorized access."[238] In addition to referencing the IP cameras' exposure of information related to children and precise geolocation information—information the FTC has traditionally recognized as sensitive[239]—the FTC also pointed to the fact that the feeds "displayed private areas of users' homes and allowed the unauthorized surveillance of . . . adults engaging in typical daily activities."[240] TRENDnet would eventually settle the case,[241] but the FTC's approach is noteworthy because it signals a willingness to consider seemingly benign information, such as video data of "adults engaging in typical daily activities," to be sensitive information if collected from within the confines of the home.[242]

Overall, questions related to the "sensitivity" of data collected, used, and retained by cloud-enabled domestic robotics could be challenging ones to answer. When looking at these questions from a categorical content perspective, the potential for debate arises when considering whether the sensitive nature of an individual's geolocation extends to the geolocation data of objects residing in a user's home. For example, companies distributing cloud-enabled domestic robots will likely attempt to limit unnecessary practices that could get in the way of a robot's functionality.[243] These companies would be inclined to argue that collecting data detailing where certain innocuous items are located within a home—such as the location of cups, furniture, fresh linens, or cleaning supplies—is much less sensitive than the location of the actual user, if at all. Consumer expectations, however, may reflect a different view. The increasing ubiquity of data generated from

---

238. *Id.* at 5. In fact, hackers were able to exploit certain vulnerabilities of TRENDnet's systems leading to "all users' live feeds to be publicly accessible." *Id.* (describing how TRENDnet's Direct Video Stream Authentication "setting failed to honor a user's choice to require login credentials and allowed all users' live feeds to be publicly accessible").

239. *See supra* note 152 and accompanying text.

240. *See* TRENDnet, *supra* note 236, at 5.

241. Press Release, Fed. Trade Comm'n, FTC Approves Final Order Settling Charges Against TRENDnet, Inc. (Feb. 7, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc.

242. *See* TRENDnet, *supra* note 236, at 5.

243. *See supra* Parts I, III.A.1.

technologies within a user's home might cause sensitivity determinations to move away from focusing on categorical content of the information and instead focus more on the location in which the information was collected, as the approach in the TRENDnet complaint seems to indicate.[244] Regardless, the need to collect linkable information combined with the sensitive nature of the home will likely raise unavoidable FIPPs issues during the advent of cloud robotics.

B. THE CONTEXT OF A CLOUD-ENABLED ROBOT TRANSACTION: DATA COLLECTION, USE, AND RETENTION LIMITATIONS

In addition to determining the application of the FIPPs based on linkable information and the rigidity of its principles based on the sensitivity of that information, companies will also need to determine the "context" in which a user discloses his or her data.[245] Under the context-centric approach many frameworks have adopted, the collection,[246] use,[247] and retention[248] limitations of data all hinge on the context in which data are originally disclosed by the user. Data practices that are considered to be within the context of a particular

---

244. *See* TRENDnet, *supra* note 236.

245. *See* WHITE HOUSE PRIVACY REPORT, *supra* note 16, at iv (explaining the FTC's approach which "focuses on the *context* of the consumer's interaction with the business") (emphasis added).

246. *See, e.g.*, WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 21 ("Companies should collect only as much personal data as they need to accomplish purposes specified under the Respect for Context principle."); 2012 FTC PRIVACY REPORT, *supra* note 17, at 27 (stating that data collection should be limited "to that which is consistent with the context of a particular transaction or the consumer's relationship with the business").

247. *See, e.g.*, WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 15 ("Consumers have a right to expect companies . . . [to] use . . . their data in ways that are consistent with the context in which consumers provide the data."); 2012 FTC PRIVACY REPORT, *supra* note 17, at 48 ("Companies do not need to provide choice[s] [when] . . . using consumer data for practices that are consistent with the context of the transaction.").

248. *See, e.g.*, WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 21 ("Companies should securely dispose of or de-identify personal data once they no longer need it."); 2012 FTC PRIVACY REPORT, *supra* note 17, at 28 (stating that companies should dispose of data "once the data has outlived the legitimate purpose for which it was collected").

transaction may be exempt, in certain circumstances, from providing choice mechanisms to consumers.[249]

"Context," like much of the terminology in the White House and FTC frameworks, is subjective in order to foster flexibility. The formal definition of context is "the circumstances that form the setting for an event, statement, or idea, and in terms of which it can be fully understood and assessed."[250] From the perspective of the frameworks at issue, a number of factors are considered when determining context, including the relationship between the company and the user, the user's age, and the user's familiarity with the technology.[251] The FTC has suggested that certain practices, such as product fulfillment and internal operations, as well as legal compliance and public purpose, provide "illustrative guidance" on practices that would be considered within the context of a data transaction.[252] In general, the context-centric approach to determining proper data practices "requires [companies] to consider carefully what consumers are likely to understand about their data practices based on the products and services they offer, how the companies themselves explain the roles of personal data in delivering them, research on consumer attitudes, and feedback from consumers."[253]

Even under this more flexible standard, however, challenges will exist for companies producing cloud-enabled domestic robots. In the world of artificial intelligence, domestic robotics moves away from a simple "closed world," where any statement not known to be true is considered false, to an "open world," where it is not yet known what piece of information is

---

249. *See, e.g.*, WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 17 (explaining how retailers may need to communicate consumers' names and addresses to fulfill shipping requests, which "is obvious from the context of the consumer-retailer relationship," and thus "do not need to provide prominent notice").

250. WORLD ECON. FORUM, UNLOCKING THE VALUE OF PERSONAL DATA: FROM COLLECTION TO USAGE 11 (2013), *available at* http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf.

251. *See, e.g.*, *supra* Part II.B.4.

252. 2012 FTC PRIVACY REPORT, *supra* note 17, at 39.

253. WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 16.

going to be useful.[254] Modern industrial robots operate in a "closed world" where they "rely on the specification of every eventuality a system will have to cope with in executing its tasks. Each response of today's robots has to be programmed in advance."[255] However, "[t]his approach is ill suited for robots in human environments, which require a vast amount of knowledge and the specification of a wide set of behaviors for successful performance."[256] The current advancements in robotics will likely resemble the move from early business computers designed to accomplish one particular service, to the more versatile personal home computer desirable for its potential and flexibility.[257] Cloud-enabled robots will be desired for similar versatility and flexibility in the form of their potential to learn. They will no longer need to operate in a "closed world," and data will no longer be limited to a single-purpose, static function.[258]

Cloud robotics, in a sense, relies on a broader, more open-ended purpose for the data it collects and uses.[259] The architecture of some cloud robotics platforms enables complex tasks to be broken down into smaller individual tasks, each of which may have previously been experienced by separate robots.[260] The data needed for a robot to grasp a particular cup in your home, for instance, may later become part of a more complex task for a robot, such as serving a drink to a particular user.[261] Data from previous experiences stored within the database would be used to assist the completion of subsequent functions that may be unrelated to the task for which the user originally disclosed the information.

---

254. *See* Raymond Reiter, *On Closed World Data Bases*, *in* LOGIC AND DATA BASES 119, 119–20 (Hervé Gallaire & Jack Minker eds., 1977), *available at* http://aitopics.org/sites/default/files/classic/Webber-Nilsson-Readings/Rdgs-NW-Reiter.pdf.

255. NICO HÜBEL ET AL., LEARNING AND ADAPTATION IN DYNAMIC SYSTEMS: A LITERATURE SURVEY 4 (2010), *available at* http://www.roboearth.org/wp-content/uploads/2011/03/D41.pdf.

256. *Id.*

257. *See Open Robotics*, *supra* note 11, at 114.

258. *Id.*

259. *See* GOLDBERG & KEHOE, *supra* note 5.

260. *Cf. id.*

261. Waibel et al., *supra* note 11, at 74 fig.5 (explaining how the "GraspBottle" task may become part of the "ServeADrink" function task).

Such broad, open-ended purposes may be unfamiliar and difficult for users to comprehend, making the "context" of any such task difficult to delineate. A disconnect may result between what users expect the context of a particular cloud-enabled robot transaction to be, and what cloud robotics actually requires in order to achieve full functionality.[262] Such a disconnect makes setting proper data collection, use, and retention limits difficult. For instance, we can imagine a world in which robots move freely throughout a home, using sensors to capture every action of a home's inhabitants in order to avoid obstacles and to function properly.[263] Bedrooms, bathrooms, and the like may be captured by a robot tasked with folding and putting away laundry, serving users breakfast in bed, or any mundane tasks society is willing to request of our robotic servants. A consumer may expect that the data collected to complete these tasks are limited to the context of the particular task requested of the robot. The company's interpretation, on the other hand, as demonstrated above, may be broader. The layout of a particular room may be useful to complete other entirely different tasks, even sharing the data with other consumers' robots to aid in future functionality.[264] For these reasons, determining the appropriate balance between meeting consumer expectations and enabling product fulfillment will be critical, yet prove to be difficult.

These difficulties may lead to inconsistent data practices among companies, which could signal an unjustifiable risk to consumer data and privacy. Such risks have been found in similar new technologies, including Internet-connected cars.[265] In a recent report to Congress, the Government Accountability Office (GAO) noted that, despite taking security measures, there is "wide variation in how long [car manufacturers, navigation device companies, and app developers] retain vehicle-specific or personally identifiable location data."[266]

---

262. *E.g.*, *id.*

263. *See id.* at 71–72.

264. *Id.* at 71–75.

265. U.S. GOV'T ACCOUNTABILITY OFFICE, IN-CAR LOCATION-BASED SERVICES: COMPANIES ARE TAKING STEPS TO PROTECT PRIVACY, BUT SOME RISKS MAY NOT BE CLEAR TO CONSUMERS (2013), *available at* http://www.gao.gov/assets/660/659509.pdf.

266. *Id.* at 16.

Additionally, "[t]o the extent that . . . identifiable data are retained, risks increase that location data may be used in ways consumers did not intend or may be vulnerable to unauthorized access."[267] These risks may be magnified in cloud robotics, where more data, with greater sensitivity, may be retained for even longer periods since it may be useful to robot performance and learning far into the future. Yet, "reasonable" restrictions on the length of time data are retained, as required by the FIPPs,[268] will prove difficult with "context" as the guide.[269]

The cloud robotics industry may also see discrepancies among companies when it comes to collection limitation and use limitation practices, both of which also rely on difficult to define "context."[270] Privacy concerns that result from the vast collection of data may be magnified due to the sheer volume of data that must be collected in order for cloud robotics to function.[271] It will be important to consider how traditionally prescribed limits on collection, if still applicable,[272] will affect cloud robotics, and whether "reasonable" limits based on context can continue to serve as an effective privacy limitation for more data-dependent machines.

Understanding the contextual scope in which a user discloses information to a cloud-enabled domestic robot could be even more complicated because of the "unique social

---

267. *Id.* at intro.

268. WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 17, 21.

269. *Id.* at 17

270. *Id.* at 16.

271. *See, e.g.*, Justin Brookman & G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm*, *in* BIG DATA AND PRIVACY: MAKING ENDS MEET 11, 11 (Future Privacy Forum & Stanford Law Sch. Ctr. for Internet & Soc'y eds., 2013), *available at* http://www.futureofprivacy.org/wp-content/uploads/Big-Data-and-Privacy-Paper-Collection.pdf (articulating five "threat models" for data collection: "data breach, internal misuse, unwanted secondary use, government access, and chilling effect on consumer behavior").

272. Policy discussions related to current technological phenomena have caused many to reconsider whether privacy frameworks should focus as they have on collection limitations. *See* FRED H. CATE ET AL., DATA PROTECTION PRINCIPLES FOR THE 21ST CENTURY: REVISING THE 1980 OECD GUIDELINES 15–16 (2013), *available at* www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf (proposing a reformed "Collection Principle" that "reflects a deliberate effort to move the focus of data protection away from data collection and the attending disclosure and consent requirements").

meaning" cloud-enabled domestic robots may have in society.[273] Robotics law scholars have noted that individuals commonly anthropomorphize robots: people name them,[274] feel sympathy and grief for them when they are mangled or destroyed,[275] and foster an overall sense of social connection with them.[276] Because of this social connection, humans are likely to interact with robots as if they are interacting with their human counterparts. "Generally speaking, the more human-like the technology, the greater the reaction."[277] University of Washington School of Law Professor and noted robotics law scholar Ryan Calo has stated, "[p]eople cooperate with sufficiently human-like machines, are polite to them, decline to sustain eye-contact, decline to mistreat or roughhouse with them, and respond positively to their flattery."[278] In many situations, this form of social acceptance is critical to robots reaching their potential as domestic servants or caregivers to their human users.[279] By making robots more engaging and socially approachable, for instance, robots will be better able to care for the elderly, the disabled, or children.[280]

Humans' willingness to interact with robots as if they were human, however, "could have a profound effect on privacy and the values it protects."[281] Human tendency to

---

273. *See Robots and Privacy*, *supra* note 12, at 194–98.

274. *See, e.g.*, *id.* at 195 (summarizing the work of technology forecaster Paul Saffo).

275. Joel Garreau, *Bots on the Ground*, WASH. POST (May 6, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/05/05/AR2007050501009.html (describing an Army colonel who halted a battle robot's exercises because the colonel could not stand to watch "the burned, scarred and crippled machine," which would blow up landmines by sacrificing its stick-insect limbs, "drag itself forward on its last leg").

276. Kate Darling, *Extending Legal Protection to Social Robots*, IEEE SPECTRUM (Sept. 10, 2012, 6:52 PM), http://spectrum.ieee.org/automaton/robotics/artificial-intelligence/extending-legal-protection-to-social-robots ("As technological progress begins to introduce more robotic toys, pets, and personal-care aids into our lives, we are seeing an increase in robots that function as companions.").

277. *Robots and Privacy*, *supra* note 12, at 195 (citing BYRON REEVES & CLIFFORD NASS, THE MEDIA EQUATION: HOW PEOPLE TREAT COMPUTERS, TELEVISION, AND NEW MEDIA LIKE REAL PEOPLE AND PLACES (1996)).

278. *Id.*

279. *See id.*

280. *Id.*

281. *Id.*

anthropomorphize robots is in part due to their unfamiliarity with the technology.[282] People are "especially inclined to assign autonomy, intent, or feelings to actions that actually result from algorithms they do not understand."[283] Because of this failure to functionally understand robots, and because of society's inclination to perceive robots as people, robots are in a unique position to elicit vast amounts of human confidences and information in ways not typical of current technologies.[284] Moreover, our interaction with these robots could reach an entirely new level of intellectual complexity, unlikely fully contemplated or even considered with our current technologies.[285] As Professor Calo has astutely hypothesized, "we stand to surface our most intimate psychological attributes" with programmable social robots, such as the potential cloud-enabled domestic robot; "[s]uddenly our appliance settings will not only matter, they also will reveal information about us that a psychotherapist might envy."[286] Overall, the complexity of these social interactions will exacerbate the challenges of understanding context for both users and cloud robotics companies.[287]

We may not soon know the full extent to which a user will be able to meaningfully understand how their data is collected, used, and retained in a world with cloud-enabled domestic robots. This may mean that it will be necessary to require companies, especially during the advent of the technology in the consumer space, to presume that consumers do not understand the data practices fundamental to cloud robotics. Unlike other technologies that have had time to develop use

---

282. Darling, *supra* note 276.

283. *Id.*

284. *See Robots and Privacy*, *supra* note 12, at 196–97.

285. *See* HEATHER KNIGHT, HOW HUMANS RESPOND TO ROBOTS: BUILDING PUBLIC POLICY THROUGH GOOD DESIGN 18 (Brookings Ctr. for Technological Innovation eds., 2014), *available at* http://www.brookings.edu/~/media/Research/Files/Reports/2014/07/29%20how%20humans%20respond%20to%20robots%20knight/HumanRobot%20PartnershipsR2.pdf ("As social robotics researchers increase their understanding of the human cultural response to robots, [they] help reveal cultural red lines that designers in the first instance, and policymakers down the road, will need to take into account.").

286. *See Robots and Privacy*, *supra* note 12, at 198.

287. *Cf. id.*

norms and customs, the "open world" design of cloud robotics[288] may be so fundamentally new, and consumer sophistication in this area may be so low, that the industry will not be able to rely on the existence of adequate contextual expectations when designing privacy practices. In addition, user interactions with robots inevitably evoke a number of social considerations, including the idea that an anthropomorphized and socially accepted robot will be able to solicit from an individual more information than other technologies.[289] These social issues must also be considered when determining the context of a transaction and how we define consumer expectations.[290] All this may mean that companies will have to rely heavily on heightened data practice disclosures and meaningful choice mechanisms, described below.

C. ADEQUATE DISCLOSURES AND MEANINGFUL CHOICES BETWEEN A CLOUD-ENABLED ROBOT AND THE USER

Simply because a particular data collection or use practice may be deemed "outside" the context of the transaction doesn't necessarily mean that a company is prohibited from collecting, using, or retaining related personal data. Instead, these frameworks call for companies to present clear and articulable disclosures of their data practices—outside of a privacy policy or other legal document[291]—and provide "meaningful" control mechanisms that allow the user to exercise choices regarding the data they disclose to companies.[292] These disclosures should include what personal data the company intends to collect, how the data will be used, and other relevant information necessary to allow the consumer to make meaningful choices about their

---

288. *See supra* notes 254–58 and accompanying text.

289. *See Robots and Privacy*, *supra* note 12, at 198 ("But the law is, in a basic sense, ill equipped to deal with the robots' social dimension.").

290. *See* WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 15 ("Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which the consumers provide the data.").

291. *E.g.*, 2012 FTC PRIVACY REPORT, *supra* note 17, at 27 (explaining that, if data collection is inconsistent with the contexts of a particular transaction, "companies should make appropriate disclosures to consumers at a relevant time and in a prominent manner—*outside of a privacy policy or other legal document*") (emphasis added).

292. *See* WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 16.

data.[293] Even if data is collected, used, and retained within the context of the transaction, the high sensitivity of that data could still require companies to disclose their data practices and provide easy access for users to exercise choices related to their data.[294] However, the time at which these choices are to be presented to the user, as well as the way in which they are presented, may create a number of challenges for cloud robotics.

1. When Meaningful Choices Are Provided

Providing adequate disclosures and choice mechanisms at a "meaningful" time may pose a number of challenges for a technology whose collection, analysis, and actuation of data can occur seamlessly without user interaction. Under the White House and FTC frameworks, choice mechanisms should be presented to a user at a time in which the consumer is able to make "meaningful" decisions about his or her data.[295] For some, the time at which a user can make meaningful decisions is at the time of, or just prior to, collection.[296] The collection-centric timeframe has typically been utilized as the preferred way to present choices to a consumer because collection, use, and disclosure practices can be halted until a user performs some action, such as affirmatively consenting to certain data practices.[297]

The nature of cloud-enabled robots, which will likely have the autonomy to seamlessly collect, disclose, and use data, may pose challenges to establishing the time in which choices can be

---

293. *See id.* at 18 ("A company should clearly inform consumers of what they are getting in exchange for the personal data they provide.").

294. *See* 2012 FTC PRIVACY REPORT, *supra* note 17, at 58–61 (examining when affirmative expressed consent is required).

295. WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 11; 2012 FTC PRIVACY REPORT, *supra* note 17, at 50 (emphasizing that the choice must be "meaningful and relevant").

296. *E.g.*, WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 11 ("*[A]t the time of collection*, companies should present choices . . . .") (emphasis added); 2012 FTC PRIVACY REPORT, *supra* note 17, at 48 ("Companies [s]hould [p]rovide [c]hoices [a]t a [t]ime and [i]n a [c]ontext in [w]hich the [c]onsumer [i]s [m]aking a [d]ecision [a]bout [h]is or [h]er [d]ata.").

297. 2012 FTC PRIVACY REPORT, *supra* note 17, at 49–50 ("In most cases, providing choice before or at the time of collection will be necessary to gain consumers' attention and ensure that the choice presented is meaningful and relevant.").

communicated to a user. Unlike certain devices, such as mobile phones that generally rely on interaction with the user to properly function, cloud-enabled robots intend to be more autonomous and less reliant on user assistance in order to collect, analyze, and act on data.[298] This autonomy may make the time of collection a less meaningful point for a user to make choices about the collection and use of his or her data. We are beginning to see the advent of autonomous household technologies today.[299] For instance, the Nest home thermostat is a self-learning, web-enabled device that learns a user's temperature preferences and automatically regulates the home environment accordingly, which can save energy and lower the cost of bills.[300] Similar to cloud-enabled robots, Nest's systems can perform certain actions without constant user interaction.[301]

Unlike devices like Nest, however, which know and communicate to the user what data will be collected and used ahead of time,[302] the data necessary to complete a cloud-enabled robot's desired function may not be known at the time the task is initiated by the user.[303] Nest, for instance, details explicitly what data the Nest Learning Thermostat will collect.[304] Cloud-enabled domestic robots' data collection and use practices, on the other hand, will likely not be so articulable and finite.[305] For instance, even the seemingly simple task of fetching a bottle of water would require "locating a bottle that contains the drink, navigating to the bottle's position on a cupboard, grasping and picking up the bottle,

298. Waibel et al., *supra* note 11, at 70–71.

299. *E.g.*, NEST, https://nest.com/ (last visited Nov. 4, 2014); *cf., e.g.*, GOLDBERG & KEHOE, *supra* note 5; *PR2: Overview*, *supra* note 2.

300. NEST, *supra* note 299.

301. *Id.*

302. *Privacy Statement*, NEST, https://nest.com/legal/privacy-statement/ (last visited Nov. 4, 2014) (detailing that the Nest Learning Thermostat will collect "[i]nformation input during setup," "[e]nvironmental data from the Nest Learning Thermostat's sensors," "[d]irect temperature adjustments to the device," "[h]eating and cooling usage information," and "[t]echnical information from the device," as well as providing details of the data that each of these categories entails).

303. *E.g.*, Waibel et al., *supra* note 11, at 70–71.

304. *Privacy Statement*, *supra* note 302.

305. *See supra* Part I.

locating the [user] . . . navigating to the [user], and giving the bottle to the [user]."[306] The robot must also be prepared to respond to the infinite, unforeseen obstacles that may be encountered along the way, making such an innocuous task even more difficult. Overall, operating in an unstructured environment may mean that the robot must adapt to situations that may be unforeseen at the time a task is requested.[307] This makes "meaningful" decision-making by a user at the time of collection much more challenging.[308]

An alternative approach, however, is worth highlighting. The FTC Framework states, "[i]n some contexts . . . it may be more practical to communicate choices at a later point."[309] Such approaches may be appropriate when "there is likely to be a delay between when the data collection takes place and when the consumer is able to contact the company in order to exercise any choice options."[310] This could be the case with cloud robotics, where robots may be expected to perform tasks around the home throughout the day while users are busy.[311] In such cases, "the company should wait for a disclosed period of time before engaging in the practices for which choice is being offered."[312] If cloud robotics were to adopt such an approach, robots could, in theory, complete a task at the user's request by collecting whatever personal or sensitive information is necessary, but refrain from using that data in connection with any other task until choices regarding future use are communicated to the user. Depending on the timing of such a choice, it could be considered "relevant" and "meaningful" for future uses or retention of that data. After all, as the FTC has said, "[d]isclosures may have little meaning for a consumer if made at one point in time, yet that same disclosure may be highly relevant if made at another point in

306. Waibel et. al., *supra* note 11, at 70.

307. *See supra* Part I.

308. *See* 2012 FTC PRIVACY REPORT, *supra* note 17, at 49 ("[W]here data collection occurs automatically . . . obtaining consent before collection could be impractical.").

309. *Id.* at 50.

310. *Id.*

311. *E.g.*, Waibel et al., *supra* note 11, at 69–71.

312. 2012 FTC PRIVACY REPORT, *supra* note 17, at 50.

time."[313] In effect, the autonomous functionality of cloud robotics will have us rethink the appropriate time to disclose relevant data practices and provide meaningful choices.

2. How Meaningful Choices Are Provided

While it is important to ask *when* relevant disclosures and choice mechanisms should be communicated to a user, it is equally important to ask *how* a company provides such notice and choice mechanisms. Many of the principles underlying the White House and FTC frameworks rely on a company's ability to interact with a consumer "in a context that is relevant to the consumer's decision about whether to allow the data collection or use."[314] For consumer-facing entities, the physical devices with which consumers interact have consistently been relied upon as the most appropriate medium for providing notices and communicating consumer choices.[315] The Consumer Privacy Bill of Rights, specifically, stresses that the disclosure of company data practices should be "easy to read *on the devices that consumers actually use to access their services*."[316] The FTC, as well, has relied on the device itself when recommending how mobile application service providers could adhere to the FTC Framework, suggesting that mobile applications accessing sensitive information "provide a just-in-time disclosure of that fact and obtain affirmative express consent from consumers" on the device.[317] This is not to say that the device is the only sufficient place to communicate data practices to a user,[318] but given its proximity and focal point of

313. FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 11 (2013), *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

314. 2012 FTC PRIVACY REPORT, *supra* note 17, 49–50.

315. WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 15.

316. *Id.* (emphasis added).

317. FED. TRADE COMM'N, *supra* note 313, at 15.

318. For instance, Mobile Location Analytics has become a popular tool used by retailers "to reduce waiting times at check-out, to optimize store layouts and to understand consumer shopping patterns" by "recognizing the Wi-Fi or Bluetooth MAC addresses of cellphones as they interact with store Wi-Fi networks." FUTURE OF PRIVACY FORUM, MOBILE LOCATION ANALYTICS: CODE OF CONDUCT 1 (2013), *available at* http://www.futureofprivacy.org/wp

interaction with the user, the device itself has been considered an appropriate medium through which to communicate relevant disclosures.[319]

Determining how to deliver meaningful choice mechanisms, especially when relying on the physical robot itself, may be challenging for cloud robotics. Cloud-enabled robots will not necessarily require an on-board user interface in order to function.[320] Computers, tablets, and mobile devices, on the other hand, typically provide screens on which to display collection and use practices, allowing "just-in-time" notifications on the screen prior to collection.[321] Cloud-enabled robots may therefore have to find alternative means through which to communicate their data practices.

A similar issue has been raised as industry begins to address the privacy challenges facing the "Internet of Things" phenomenon—which is "the concept that the Internet is no longer just a global network for people to communicate with one another using computers, but it is also a platform for devices to communicate electronically with the world around them."[322] Internet-connected cars, for instance, provide a helpful example. During a recent FTC workshop on the Internet of Things, commenters raised concerns over how to adequately disclose data practices and provide choice

---

-content/uploads/10.22.13-FINAL-MLA-Code.pdf. The Future of Privacy Forum's Code of Conduct for retailers utilizing Mobile Location Analytics proposes that notice, when required, should be provided to store patrons through "signage that informs consumers about the collection and use of MLA Data at that location." *Id.* at 1–2.

319. *See* WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 14–15 (emphasizing that the device is a good place for the notice, using mobile devices as an example).

320. For instance, AMIGO, a domestic service robot created at the Eindhoven University of Technology, was used to demonstrate RoboEarth, and did so without an on-board user interface. *See* TechUnited Eindhoven, *AMIGO Robot Downloads Its Instructions from the RoboEarth Internet!*, YOUTUBE (Feb. 1, 2011), http://www.youtube.com/watch?v=RUJrZJyqftU; *Robots/AMIGO*, ROS.ORG, http://wiki.ros.org/Robots/AMIGO (last visited Nov. 4, 2014).

321. FED. TRADE COMM'N, *supra* note 313, at 15–18 (providing examples of iOS and Android devices and their methods of notification).

322. *See, e.g.*, DANIEL CASTRO & JORDAN MISRA, CTR. FOR DATA INNOVATION, THE INTERNET OF THINGS 2 (2013), *available at* http://www2.datainnovation.org/2013-internet-of-things.pdf.

mechanisms for products that lack a user interface.[323] In response to these concerns, commenters such as the American Automobile Association (AAA) suggested that connected car automakers and service providers that could not feasibly integrate a dashboard user interface into their vehicles could provide "websites or other online services that explain car data practices, educate consumers and, in turn, allow them to make choices about those practices."[324] AAA also suggested that connected cars "could communicate with consumers via email, phone, or text message (provided the user agrees to such communications)."[325] In attempting to comply with the FIPPs, cloud robotics could find these examples useful.

However, causing an additional hurdle for cloud-enabled robots, one which many Internet of Things products may not face, is the fact that cloud-enabled robots are likely to be highly autonomous, which entails performing relatively unpredictable movements.[326] While there is no universally accepted definition of "robot,"[327] a defining characteristic that is considered in a number of proposed definitions is the ability of the machine to have autonomous mobility.[328] When envisioning a world in which robots conduct domestic tasks such as doing the laundry, making the bed, cleaning a room, or doing the dishes, the ability of the robot to move seamlessly throughout its environment is important. But in a circumstance in which a

---

323. Letter from Daniel W. Caprio Jr., Senior Strategic Advisor, Transatlantic Computing Continuum Policy Alliance, to Donald S. Clark, Sec'y, Fed. Trade Comm'n (Jan. 10, 2014), *available at* http://www.ftc.gov/sites/default/files/documents/public_comments/2014/01/00017-88305.pdf ("Some IoT devices will employ user interfaces which will clearly indicate to individuals how data is being collected and may offer controls . . . [while] other technologies will collect and transfer data with little to no recognizable interface . . . .").

324. Letter from Gerard J. Waldron & Stephen P. Satterfield, Counsel, AAA, to Donald S. Clark, Secretary, Fed. Trade Comm'n (Jan. 10, 2014), *available at* http://www.ftc.gov/sites/default/files/documents/public_comments/2014/01/00012-88249.pdf.

325. *Id.*

326. *E.g.*, Robert Speer et al., *The GAUDI Project: Design and Development Issues in Constructing an Intelligent Robot*, COMPLEXITY INT'L (Apr. 2006), http://www.complexity.org.au/ci/vol03/gaudi2/gaudi2.html (describing a robot with a high degree of freedom which would learn with independent neural networks).

327. Denning et al., *supra* note 15, at 105.

328. *Id.* at 105–06.

cloud-enabled robot happens upon sensitive data that would require consumer choices or consent, it is likely that the user may be nowhere near the robot, as they could be in another room or outside of the house entirely.

Thus, cloud-enabled robots that are both highly mobile and unpredictable may require companies to find a method for communicating data practices and providing meaningful choices in a context not dependent upon the physical robot itself. RoboEarth's architecture, for instance, does support a web interface platform "that allows humans to exchange information with the [RoboEarth] database using hypertext mark-up language (HTML) forms."[329] Similar to AAA's suggestion in the connected car context,[330] RoboEarth's web interface could potentially allow individuals to access privacy notices, and in certain situations provide an opportunity for a consumer to consent to the collection of sensitive data.[331] Overall, cloud-enabled robots may prove to be fertile ground for new understandings of how to properly provide relevant disclosures and meaningful choices to consumers.

D. TRANSPARENCY & PRIVACY NOTICES

In addition to providing disclosure of specific data practices so consumers can make meaningful choices, producers of cloud-enabled domestic robots may also experience difficulties in properly disclosing general information about company practices.[332] Regardless of the sensitivity of data collected by an entity, or the context of a particular transaction, companies should provide descriptions of privacy and security practices in a conspicuous location for privacy-conscious users.[333] Recent privacy frameworks have recognized some of the shortcomings

---

329. Waibel et al., *supra* note 11, at 75.

330. Letter from Gerard J. Waldron & Stephen P. Satterfield to Donald S. Clark, *supra* note 324, at 9.

331. *Cf.* Waibel et al., *supra* note 11, at 75.

332. *See* WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 14 ("[C]ompanies should provide clear descriptions of what personal data they collect, why they need the data, how they will use it, when they will delete the data or de-identify it from consumers, and whether and for what purposes they may share personal data with third parties.").

333. *E.g.*, 2012 FTC PRIVACY REPORT, *supra* note 17, at 50 (specifying that the method of notice could be "directly adjacent to where the consumer is entering data").

of traditional privacy notices,[334] and have called for companies to provide notice of their data practices in a manner that is "easily understandable" and which should be "clearer, shorter, and more standardized."[335] Determining how to properly articulate the complex data practices for a cloud-enabled robot in a manner that is easy to understand, clear, and short, however, may prove difficult.

To begin with, privacy notices for cloud-enabled domestic robots will face problems similar to those discussed above when determining how to disclose data practices in order to provide meaningful choice mechanisms.[336] Disclosures will unlikely be able to communicate with any specificity the data that will be collected, or the manner in which they may be used, due to the autonomous nature of cloud-enabled robots operating in unstructured environments.[337] Additionally, efforts to make these notices clearer, shorter, and more standardized could leave out important practices that should be communicated to users, reflecting what some call the "transparency paradox."[338]

Companies producing cloud-enabled domestic robots will also need to be wary of describing practices in broad terminology in an attempt to make sure that all practices are covered.[339] Modern technologies are currently struggling with this problem.[340] The GAO report, described above, also found that automobile manufacturers, portable navigation device companies, and developers of map and navigation applications for mobile devices "have taken steps"[341] to adopt industry-

---

334. *E.g.*, Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S J.L. & POL'Y INFO. SOC'Y 425, 428 (2011) (describing some of the criticisms of the "informed consent model," including the fact that privacy notices are "largely unread, not very informative, and written too broadly").

335. 2012 FTC PRIVACY REPORT, *supra* note 17, at 64; *see also* WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 14.

336. *See supra* Part III.C.1.

337. *See, e.g.*, Waibel et al., *supra* note 11 (showing that RoboEarth's cloud robot architecture necessitates gathering information spontaneously and continuously).

338. Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DÆDALUS 32, 36 (2011).

339. *E.g.*, U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 265, at 13 (criticizing the use of broad wording).

340. *Id.*

341. *Id*. at 12.

recommended privacy practices, but "the companies' privacy practices were, in certain instances, unclear, which could make it difficult for consumers to understand the privacy risks that may exist."[342] The GAO took exception, for instance, to the fact that in most companies' disclosures, "the stated reasons for collecting location data were not exhaustive," but rather "broadly worded."[343] Companies producing cloud-enabled robots may find it infeasible to offer an "exhaustive" list of possible data collection, use, and retention practices, but may be criticized if they communicate practices with broad terminology.

The advent of cloud robotics, however, may provide an opportunity for notice practices to move beyond the traditional approaches and instead experiment with alternative, more effective means of disclosure.[344] The FTC has urged more standardization, allowing users to more easily compare policies and to provide consistency among the many methods used to communicate the same data practices.[345] Early efforts to standardize cloud robotics privacy notices could allow companies producing cloud-enabled domestic robots to avoid the pitfalls of varying and incoherent clauses. Others have advocated moving away from using "text and symbols" to provide notice, and instead, conducting more research on "a new generation" of notice.[346] The adoption of "visceral notice," for instance, in which physical sensations and experience communicate information to a user, may be a unique and effective approach for cloud-enabled robots to provide notice to users of data collection and use practices.[347]

---

342. *Id.*

343. *Id*. at 12–13.

344. *E.g.*, Letter from Gerard J. Waldron & Stephen P. Satterfield to Donald S. Clark, *supra* note 324, at 9 (putting forth websites and email as one type of effective disclosure).

345. *See* 2012 FTC PRIVACY REPORT, *supra* note 17, at 61–63 (discussing types of forms which may be used to standardize notices).

346. M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1030 (2012) ("[This Article] argues against an extreme skepticism of mandatory notice . . . by questioning whether critics or proponents of notice have identified and tested all of the available notice strategies.").

347. *Id.* at 1034–46 (examining possible ways to deliver visceral notices).

E. SECURITY

While the data security challenges posed by cloud robotics may be similar to other technologies, the sensitivity of data collected, used, and retained by cloud-enabled robots will likely place added pressure on companies to secure their data.[348] The White House and FTC frameworks call for some form of "reasonable" or "responsible" data security practices.[349] That said, many frameworks intentionally refrain from stating what specific security practices would qualify as "reasonable" or "responsible," and instead highlight that industry best practices and standards would provide the basis for reasonable security practices.[350] Some states have established reasonable data security practices through regulation,[351] while the FTC has highlighted "reasonable" and "appropriate" practices within its Section 5 complaints against companies accused of "unfair" and "deceptive" data security practices.[352] Many entities have also developed their own technology-centric approaches to data security.[353] Cloud robotics will likely be able to adopt existing security standards,[354] but the sensitivity of data collected, used,

---

348. *See Robots and Privacy*, *supra* note 12, at 194 (explaining that, unlike security vulnerabilities with traditional devices, home robots "can move and manipulate, in addition to record and relay," allowing "a robot hacked by neighborhood kids . . . [to] vandalize a home or frighten a child or elderly person").

349. WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 19; 2012 FTC PRIVACY REPORT, *supra* note 17, at 24–26.

350. WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 19 (recognizing that the Consumer Privacy Bill of Rights "Security" principle "gives companies the discretion to choose technologies and procedures that best fit the scale and scope of the personal data that they maintain").

351. *See, e.g.*, MASS. GEN. LAWS ANN. ch. 93H, § 2 (West 2007); 201 MASS. CODE REGS. 17.03 (2007) (detailing requirements for reasonable data security).

352. *See, e.g.*, TRENDnet, *supra* note 236, at 4 ("[TRENDnet] failed to employ reasonable and appropriate security in the design and testing of the software that it provided consumers for its cameras.").

353. *See e.g.*, FUTURE OF PRIVACY FORUM & CTR. FOR DEMOCRACY & TECH., BEST PRACTICES FOR MOBILE APPLICATION DEVELOPERS 12–13 (2012), *available at* https://www.cdt.org/files/pdfs/Best-Practices-Mobile-App-Developers.pdf (proposing standard security practices for mobile app developers).

354. For instance, RoboEarth states that its data are "made available via standard Internet protocols." Waibel et al., *supra* note 11, at 71.

and retained by cloud-enabled robots could very well make the consequences of any compromised cloud robot network or database so significant that companies would be required to go beyond current best practices.[355] As cloud robotics continues to advance, relevant trade associations dealing in robotics may begin to recognize some of the nuanced security risks that a cloud environment for robots might create, and develop security standards accordingly.[356]

F. ACCESS & ACCURACY

Companies producing cloud-enabled domestic robots will also need to determine how they can maintain the accuracy of the data they collect, as well as the extent to which users can access the data collected and stored.[357] Privacy frameworks generally include access and accuracy practices in which companies determine the appropriate extent of user access to data based upon data sensitivity and impact on the user.[358] The right to access has been a core of the FIPPs since first articulated within the Department of Health, Education, and Welfare Report.[359] However, the increasing ubiquity of data has caused many to rethink the extent to which access should be provided to users.[360]

While some have found that increased access to data, regardless of the technology, is critical "[i]n an environment

---

Contemporary encryption methods and similar security practices for such protocols could be utilized within the cloud architecture.

355. *See Robots and Privacy*, *supra* note 12, at 196–97 (stating that robots can elicit information in ways not typical of current technologies).

356. Such an approach could follow approaches taken within other areas of robotics. *See, e.g.*, *New Robot Safety Standards*, ROBOTIC INDUSTRIES ASS'N (May 29, 2013), http://www.robotics.org/content-detail.cfm/Industrial-Robotics-News/New-Robot-Safety-Standard/content_id/4133 (establishing "American national robot safety standard[s]" for robot manufacturers and integrators).

357. WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 19 ("Consumers have a right to access and correct personal data.").

358. *Id.*

359. DEP'T OF HEALTH, EDUC. & WELFARE, *supra* note 68, at xx.

360. *E.g.*, THOMAS M. LENARD & PAUL H. RUBIN, THE BIG DATA REVOLUTION: PRIVACY CONSIDERATIONS 20 (Tech. Policy Inst. ed., 2013), *available at* https://www.techpolicyinstitute.org/files/lenard_rubin_thebigdata revolutionprivacyconsiderations.pdf (pointing out the incentive for modifying information inaccurately for one's own ends).

where consent is not always possible or feasible,"[361] others are less persuaded by the benefits to the user of doing so.[362] As cloud robotics becomes more advanced, the industry may need to understand not only how information is to be collected and analyzed by a robot, but also the impact that information will have on the user.[363] While inaccurate information in the robot database may not be as harmful as inaccurate credit information, the impact could still be significant. Providing users access to data collected and stored within a cloud-robot database would not only satisfy access principles, but could also provide users with an increased level of control over the data.[364]

G. ACCOUNTABILITY

Finally, maintaining accountability may be problematic for companies producing cloud-enabled domestic robots because, as detailed in this Section, it is still unknown which practices the consumer cloud robotics industry will need to emphasize in order to comply with the FIPPs. The principle of accountability requires companies to be accountable for complying with their respective FIPPs framework.[365] Yet, as some have observed, creating and enforcing accountability "is increasingly difficult given the external pressure for increased flexibility in design of rules."[366] With so many frameworks emphasizing different principles, "[t]he challenge surrounding accountability focuses both on which principles to support as well as how to effectively uphold and enforce them."[367] Proper accountability will only be possible if companies producing cloud-enabled domestic robots and relevant stakeholders understand and collectively agree on

---

361. David A. Hoffman, *Putting Privacy First in Big Data Technologies*, RE/CODE (Feb. 10, 2014, 4:00 AM), http://recode.net/2014/02/10/putting-privacy-first-in-big-data-technologies/.

362. *See* LENARD & RUBIN, *supra* note 360, at 20.

363. WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 19–20 (stating companies should consider the possible harms that could befall a consumer).

364. Such access to databases has already started to occur within cloud robotic infrastructures. RoboEarth's user interface, for instance, would allow users to view information uploaded onto the RoboEarth database. SCHIEßLE ET AL., *supra* note 218, at 15.

365. *E.g.*, WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 21–22.

366. WORLD ECON. FORUM, *supra* note 250, at 17.

367. *Id.* at 3.

how best to adhere to the frameworks. Once effective practices are in place, accountability practices such as audits, evaluations, and privacy impact assessments will need to be utilized in order for cloud robotics companies to determine what specific privacy objectives are required or desired, and whether or not those objectives have been achieved.[368]

IV. APPROACHING THE PRIVACY CHALLENGES INHERENT IN CONSUMER CLOUD ROBOTICS

By examining the FIPPs and recent privacy frameworks, and applying those approaches to cloud-enabled domestic robots, we can begin to see some of the challenges that lay ahead for companies wishing to experiment with this innovative technology. But the lingering abstract question many may be asking is, "why now?" Why should policymakers and roboticists consider how today's consumer privacy frameworks will affect cloud robotics—a concept that is still some time away from being as ubiquitous as smartphones or personal computers? The answer, in part, lies in the belief that society can be better prepared to address and mitigate consumer privacy challenges the earlier these challenges are discovered and understood.[369] By recognizing the possible inconsistencies that may result from applying these frameworks to cloud robotics concepts, companies can have the advantage of easily adjusting, amending, or emphasizing certain practices in order to respect consumer privacy.[370] An ounce of prevention, as they say, is worth a pound of cure.

Recognition of these challenges, however, does not necessarily require finding immediate solutions. A productive future starts with asking the right questions. Tamara Denning

---

368. *E.g.*, WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 21 ("Where appropriate, companies should conduct full audits.").

369. *See, e.g.*, *Rethinking Personal Data*, WORLD ECON. FORUM, http://www.weforum.org/projects/rethinking-personal-data (last visited Jan. 18, 2015) (explaining the World Economic Forum's project to examine and understand contemporary commercial data practices in order to "facilitate the creation of a trusted, transparent and user-centred personal data ecosystem").

370. *See* Denning et al., *supra* note 15, at 105 (arguing that "now is the ideal time" to research potential security and privacy risks associated with household robots, "while the field of household robotics is comparatively young and before robots with serious and fundamental security flaws become ubiquitous").

and co-authors from the University of Washington and Intel Labs, for instance, recently examined some of the privacy and security flaws of modern household robots.[371] The research uncovered significant security vulnerabilities that could allow an attacker to intercept or inject wireless packets into some of the tested household robots.[372] After synthesizing the results, the authors "identif[ied] a set of questions capable of isolating key social, environmental, and technical properties of the robot in question" and "provide[d] a core set of questions to identify how the robot's properties might affect the security and privacy of users and their property."[373] Some of these proposed questions are basic design questions, such as "[h]ow mobile is the robot"[374] and "[w]hat is the robot's intended operational environment,"[375] while more complex questions include, "[d]oes the robot create new or amplify existing privacy vulnerabilities?"[376]

An approach similar to Denning's method of recognizing the challenge[377] and presenting questions and suggestions[378] to overcome privacy concerns could prove valuable not only from a design perspective, but from a law and policy perspective. Consider, for example, the frameworks' focus on "context."[379] As this Article has explained, understanding the context in which a user may disclose their data at the advent of cloud robotics may be extremely difficult, yet this is a significant component in recent privacy frameworks.[380] By recognizing this issue now, ample opportunity exists for companies to start considering what users might expect a cloud-enabled domestic robot to do with collected data, as well as understanding the many other factors that shape contextual integrity.[381]

---

371. *See* Denning et al., *supra* note 15, at 106–10.
372. *Id.* at 107–09.
373. *Id.* at 112–13.
374. *Id.* at 112.
375. *Id.*
376. *Id.* at 113.
377. *Id.* at 105.
378. *Id.*
379. WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 15–18; 2012 FTC PRIVACY REPORT, *supra* note 17, at 27.
380. *See supra* Part III.B.
381. *Cf.* 2012 FTC PRIVACY REPORT, *supra* note 17, at 38 ("This new 'context of the interaction' standard is similar to the concept suggested by

Existing research could provide an adequate starting point. Research conducted by the International Institute of Communications (IIC), for instance, examined the factors that "impact individuals' sensitivity to the collection, access, and use of their personal data" in an effort to assist policymakers in developing data management frameworks that more accurately reflect the emerging market.[382] The study identifies variables that impact a user's sensitivity to how their data are used, including, but not limited to, the type of data being accessed or shared, the type of entity with which the user interacted, the user's trust in the service provider, the method of collection, and the device used.[383]

Such qualitative research on what variables affect a user's sensitivity to data usage can greatly assist in formulating context-centric parameters to cloud-enabled robots' data collection, use, and retention practices.[384] For instance, in the IIC study, users displayed a concern over "passively collected data," or the automatic collection of data with which the users will not be involved, as opposed to "actively collected data," or data that are directly volunteered by the user.[385] The study suggests, however, that many will be more accepting of passive data collection if "they trust the service provider collecting the data," "they are able to negotiate the value exchanged for their data," "they are provided with clear insights into how the data is being collected and how it is being used," and "they have control over the types of data being collected, accessed and used."[386] Considering the dependence cloud robotics will have on passively collected data,[387] such recommendations could be a

---

some commenters that the need for choice should depend on reasonable consumer expectations.").

382. INT'L INST. OF COMMC'NS, PERSONAL DATA MANAGEMENT: THE USER'S PERSPECTIVE 5 (2012), *available at* http://www.iicom.org/open-access-resources/doc_details/264-personal-data-management-the-user-s-perspective-pdf-report.

383. *Id.* at 15–23.

384. *Cf. id.* at 40 ("Current regulatory frameworks do not consider all aspects of personal data collection and management . . . . [T]here are variables that affect the data context and these in turn, impact user sensitivity regarding personal data.").

385. *Id.* at 12–13, 20–21.

386. *Id.* at 22.

387. *See supra* Part I.

starting point for discussion as companies contemplate how cloud-enabled robots may emerge as a consumer product. By recognizing how policymakers approach consumer privacy, companies developing innovative products, like cloud-enabled robots, can begin to recognize particular challenges posed by these approaches, and guide development of both cloud robotics and its cloud architecture.

Going forward, collaboration between policymakers, privacy professionals, and the robotics community will be essential as cloud robotics continues to mature and additional consumer privacy challenges begin to arise.[388] Individuals within the robotics community should become familiar with the "heated debate" over current U.S. information privacy law.[389] Some regulators and advocates are continuously calling on Congress to propose legislation that would "close the gaps" within consumer privacy.[390] Others, however, are against any regulatory reform and believe industry self-regulation would be sufficient.[391] It is doubtful that many of the proponents of either side of the debate have sufficiently considered—or even heard of—cloud robotics. The robotics community's entrance into the law and policy discussion on privacy would provide a unique and critical perspective on tomorrow's technologies and avoid hindering the cloud robotics infrastructure.[392]

---

388. *See* WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 33 (calling for a multi-stakeholder approach to regulation); 2012 FTC PRIVACY REPORT, *supra* note 17, at 72–73 ("The FTC recommends that Congress consider baseline privacy legislation while industry implements the final privacy framework through individual company initiatives and through strong and enforceable self-regulatory initiatives.").

389. *See* Bamberger & Mulligan, *supra* note 81, at 254–63.

390. *E.g.*, Julie Brill, Comm'r, Fed. Trade Comm'n, Address at the Woodrow Wilson School of Public and International Affairs: Big Data and Consumer Privacy: Identifying Challenges, Finding Solutions (Feb. 20, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/202151/140220princetonbigdata_0.pdf ("I believe adoption of baseline privacy legislation for the commercial arena would close the gaps in consumer privacy protections and help level the playing field among businesses.").

391. *See* Adam Thierer, *Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle*, 14 MINN. J.L. SCI. & TECH. 309, 385–86 (2013).

392. Such a "call to arms" has started in the Big Data context. During FTC Commissioner Julie Brill's Sloan Cyber Security Lecture at the Polytechnic Institute of NYU, Commissioner Brill proclaimed a "call to keyboard" to engineering students, professors, company chief technology officers, and

Understanding the current privacy debate on a legal and policy level can assist roboticists in better designing privacy into cloud-enabled robots. Specifically, "Privacy by Design" advocates a systematic and proactive approach to privacy, in which privacy is "embed[ed] . . . into information technologies, business practices, and networked infrastructures, as a core functionality, right from the outset."[393] Software developers and roboticists who have a solid understanding of what practices can mitigate consumer privacy concerns from a law and policy perspective will be better positioned to design and develop cloud-enabled robots that respect these practices. Some have already advocated the introduction of privacy by design practices into robotics,[394] and consideration of such practices within cloud robotics specifically could be equally beneficial.

Additionally, advocates, policymakers, regulators, and lawyers interested in addressing the privacy concerns of emerging technologies should take heed of the advancements occurring in robotics.[395] Growth in this area is well underway.[396] A number of law firms have begun to invest in practice areas focusing on robotics.[397] The "We Robot"

---

computer scientists "to help create technological solutions to some of the most vexing privacy problems presented by big data." Julie Brill, Comm'r, Fed. Trade Comm'n, Lecture at the Polytechnic Institute of New York University: A Call to Arms: The Role of Technologists in Protecting Privacy in the Age of Big Data (Oct. 23, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/call-arms-role-technologists-protecting-privacy-age-big-data/131023nyupolysloanlecture.pdf.

393. ANN CAVOUKIAN, OPERATIONALIZING PRIVACY BY DESIGN: A GUIDE TO IMPLEMENTING STRONG PRIVACY PRACTICES 8 (2012), *available at* http://www.privacybydesign.ca/content/uploads/2013/01/operationalizing-pbd-guide.pdf. The FTC Framework explicitly advocates a "Privacy By Design" approach. 2012 FTC PRIVACY REPORT, *supra* note 17, at 22.

394. Podsiadła, *supra* note 22, at 4.

395. *E.g.*, *RobotShop Among the Fastest Growing Companies in Canada, 3rd Year in a Row*, ROBOTSHOP (June 12, 2014), http://www.robotshop.com/blog/en/robotshop-among-fastest-growing-companies-canada-3rd-year-row-13494.

396. *See. e.g.*, *id.*

397. *See, e.g.*, *Robotics, AI and Automation*, LITTLER.COM, http://www.littler.com/practice-areas/robotics-ai-and-automation (last visited Nov. 4, 2014) (focusing its practices on robotics within a workplace environment); *Robotics and Artificial Intelligence: Emerging Issues in Robotics Law*, COOKE KOBRICK & WU, http://www.ckwlaw.com/practice-areas/Robotics_and_Artificial_ Intelligence/ (last visited Nov. 4, 2014); *see also* M. Ryan Calo, *Even (Some) Law Firms Think Robots Are the Next Big Thing*,

conference, now planning its fourth event, has started to encourage discussion and collaboration on the law and policy issues surrounding robotics.[398] The American Bar Association Section of Science & Technology Law has also formed an Artificial Intelligence and Robotics Committee.[399] In addition, legal scholars have begun to contribute meaningful scholarship to the robotics field, not as satirical hypotheticals, but as meaningful contributions to discussions of how robotics will begin to adapt to our country's legal landscape.[400]

Collaboration will help recognize the privacy concerns of cloud robotics while providing a better understanding of how consumer privacy frameworks can meaningfully address potential concerns associated with cloud-enabled robots. As Peter Swire and Annie Anton have stated, "[o]rganizations today need to have both lawyers and engineers involved in privacy compliance efforts. An increasing number of laws, regulations, and cases, often coming from numerous states and countries, place requirements on companies. Lawyers are needed to interpret these requirements. Engineers are needed to build the systems."[401]

These words are especially fitting when thinking about the future of cloud robotics and privacy. Lawyers and privacy professionals may better assist in implementing appropriate privacy frameworks, or in providing alternative policy approaches to protecting user privacy, once they understand how cloud robotics is implemented, developed, and maintained. Roboticists and technologists can avoid thinking of "privacy" as

---

FORBES (Jan. 31, 2014, 1:14 AM), http://www.forbes.com/sites/ryancalo/2014/01/31/even-some-law-firms-think-robots-are-the-next-big-thing/.

398. *See* Michael Froomkin, WE ROBOT (Nov. 23, 2013), http://robots.law.miami.edu/.

399. *See Section of Science & Technology Law: Artificial Intelligence and Robotics Committee*, AM. BAR ASS'N (Oct. 24, 2014), http://apps.americanbar.org/dch/committee.cfm?com=ST248008.

400. *See, e.g.*, Dan Terzian, *The Right to Bear (Robotic) Arms*, 117 PENN ST. L. REV. 755, 770–73 (2013) (examining the Second Amendment implications of robotic weapons and robots wielding firearms); *Open Robotics*, *supra* note 11 (examining the commercial implication of "open" or "closed" robotics).

401. Peter Swire & Annie Anton, *Engineers and Lawyers in Privacy Protection: Can We All Just Get Along?*, PRIVACY PERSP. (Jan. 31, 2014), https://privacyassociation.org/news/a/engineers-and-lawyers-in-privacy-protection-can-we-all-just-get-along/.

simply preventing disclosure, and can begin to improve internal systems and focus on privacy-enhancing technologies that respect and adhere to the FIPPs. Given the complexities of both cloud robotics and privacy law and policy, collaboration may not just be beneficial, but essential to the cloud-enabled robot marketplace.

CONCLUSION

Cloud robotics proposes a unique system architecture that offloads data processing and storage onto remote servers,[402] which would allow robots to be lighter, cheaper, and more efficient in interacting within unstructured, open environments.[403] As cloud robotics continues to advance,[404] it may provide the foundation for affordable, domestic robots capable of providing a multitude of everyday services, particularly within our homes. However, the advent of cloud-enabled robots will come with a number of legal, technical, societal, and of course, privacy challenges. Consumer protection in the United States today involves a commingling of sector-specific regulations and proposed industry best practices founded on the FIPPs. Although recent privacy frameworks, including the White House Consumer Privacy Bill of Rights[405] and the FTC Framework,[406] have attempted to properly balance consumer expectations with appropriate respect to advancements in technology, challenges will likely arise when these frameworks are applied to an emerging technology like cloud robotics.

This Article identifies several questions that begin to arise as more data become necessary for cloud-enabled robots to

---

402. GOLDBERG & KEHOE, *supra* note 5.

403. Waibel et al., *supra* note 11, at 70.

404. July 2014, for instance, saw the release of the "World's First Family Robot," Jibo, "an always-connected device that automatically stores its data in the JIBO cloud." *Jibo*, *World's First Family Robot*, INDIEGOGO, https://www.indiegogo.com/projects/jibo-the-world-s-first-family-robot (last visited Nov. 4, 2014). In addition, August 2014 saw the launch of RoboBrain, "a massive online 'brain' that can help all robots navigate and even understand the world around them." Daniela Hernandez, *The Plan to Build a Massive Online Brain for All the World's Robots*, WIRED (Aug. 25, 2014, 9:00 AM), http://www.wired.com/2014/08/robobrain/.

405. WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 47–48.

406. 2012 FTC PRIVACY REPORT, *supra* note 17, at 22–32.

operate in unstructured environments. What data collected by a cloud-enabled robot would be classified as "sensitive" data? Additionally, for a technology that emphasizes the pooling, sharing, and reusing of data in order to operate,[407] what exactly will determine the limits on data collection, use, and retention practices? When and how can companies communicate "meaningful and relevant"[408] choices and disclosures to users when it might not be known what information a particular task may require, or where the user might be when the robot collects or uses data? Posing these questions helps individuals recognize that today's decisions will affect tomorrow's technologies, and should serve as an invitation to begin collaboration between the privacy and robotics communities.

407. *See* Waibel et al., *supra* note 11.

408. WHITE HOUSE PRIVACY REPORT, *supra* note 16, at 11; 2012 FTC PRIVACY REPORT, *supra* note 17, at 50 (emphasizing that the choice must be "meaningful and relevant").