Consumer Cloud Robotics and the Fair Information Practice Principles

ANDREW PROIA* DREW SIMSHAW ** & DR. KRIS HAUSER***

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,[4] 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. What Hickman was demonstrating 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 sharing of vast data resources."[5]

* 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. The author's would like to thank Dr. David Crandall and Dr. Selma Šabanović for their invaluable insight and contributions to numerous roundtable discussions that formed the basis for this Paper.

** 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.

*** Assistant Professor, Indiana University School of Informatics and Computing, Ph.D in Computer Science, Stanford University, 2008, B.A. in Computer Science & B.A. in Mathematics, University of California at Berkeley, 2003.

[1] *See* Google Developers, *Google I/O 2011: Cloud Robotics, ROS for Java and Android*, YouTube (May 11, 2011), http://www.youtube.com/watch?v=FxXBUp-4800.

[2] See *PR2: Overview*, WILLOW GARAGE, http://www.willowgarage.com/pages/pr2/overview (last visited March 5, 2014); *Software: Overview*, WILLOW GARAGE, http://www.willowgarage.com/pages/software/overview (last visited March 5, 2014).

[3] Google Developers, *supra* note 1.

[4] *Id.*

[5] *See* Ken Goldberg, *Cloud Robotics and Automation*, http://goldberg.berkeley.edu/cloud-robotics/ (last visited March 5, 2014).

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 of cloud storage providers (e.g., Dropbox, Google Drive, Apple iDrive), computation providers (e.g., Amazon EC2, Microsoft Azure), and computational paradigms (e.g., Google MapReduce, Hadoop) becoming commonplace. Similar infrastructure advances for cloud-enabled robots are beginning to take shape, and with the International Federation of Robotics estimating that personal and domestic robot sales will reach over 15 million units and be valued at over $5 billion between 2013 and 2016,[7] 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 we equate cloud-enabled robots with mainstream tech devices like smartphones, tablets, and computers. As the creators of RoboEarth, a popular cloud robot architecture, have suggested, many legal,[8] moral,[9] safety,[10] and technical[11] questions still remain as the practice of operating in unstructured environments and sharing data among robots

[6] *See* Masayuki Inaba, Satoshi Kagami, Fumio Kanehiro, Yukiko Hoshino & Hirochika Inoue, *A Platform for Robotics Research Based on the Remote-Brained Robot Approach*, 19 INT'L J. ROBOTICS RES. 933 (2000) (proposing a framework for "the remote-brain robot approach").

[7] Executive Summary, International Federation of Robotics, *World Robotics 2013—Service Robots*, at 18-19, Sept. 18 2013, *available at* http://www.ifr.org/uploads/media/Executive_Summary_WR_2013_01.pdf.

[8] *See* Markus Waibel, Michael Beetz, Javier Civera, Raffaello D'Andrea, Jos Elfring, Dorian Gálvez-López, Kai Häussermann, Rob Janssen, J.M.M. Montiel, Alexander Perzylo, Björn Schießle, Moritz Tenorth, Oliver Zweigle, & René van de Molengraft, *A World Wide Web for Robots—RoboEarth*, 2011 IEEE ROBOTICS & AUTOMATION MAG. 69, 71 (2011) (citing Calo, *infra* note 170).

[9] *See id.* (citing Calo, *infra* note 15).

[10] *See id.* (citing K. Ikuta, H. Ishii & M. Nokata, *Safety Evaluation Method of Human-Care Robot Control*, 22 INT'L J. ROBOTS RES. 281 (2003)).

[11] *See* D. Lorencik & P. Sincak, *Cloud Robotics: Current Trends and Possible Use As A Service*, *in* IEEE 11TH INT'L SYMP. ON APPLIED MACHINE INTELLIGENCE & INFORMATICS 85, 85 (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.").

integrates into our everyday lives. One "open question" in particular is what affect cloud-enabled consumer robotics, particularly domestic service robots,[12] will have on consumer privacy.

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."[13]A number of recent attempts to provide meaningful and standardized consumer privacy protections have resulted in "privacy frameworks" that intend to balance technological innovation with reasonable data collection, use, and retention limits. Underlying a majority of these frameworks are a set of practices, first articulated in the 1970s, that addresses how personal information should be collected, used, retained, and managed, known as the Fair Information Practice Principles ("Fair Information Practices" or "FIPPs"). The FIPPs have been adopted, in some form or another, by numerous national and international entities as the foundational framework for both the public and private sectors to protect the privacy and integrity of personally identifiable information. However, with cloud robotics looking to create a world in which independent machines "pool," "share," and "reuse" data,[14] the integration of interconnected robotics into our everyday lives could pose numerous challenges in adapting to a FIPPs-based framework.

[12] This Paper 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, Cynthia Matuszek, Karl Koscher, Joshua R. Smith & Tadayoshi Kohno, *A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons*, *in* UBICOMP '09 THE 11TH INTERNATIONAL CONFERENCE ON UBIQUITOUS COMPUTING 105, 105–106 (2009).
[13] WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL ECONOMY 5 (2012) [hereinafter WHITE HOUSE PRIVACY REPORT].
[14] *See, e.g.*, Waibel et. al., *supra* note 8, at 70; Goldberg, *supra* note 5.

The privacy implications of robotics have been addressed from both a legal and technical perspective.[15] However, we lack an understanding of how current standards and proposed frameworks for protecting consumer privacy may affect the future of robotics as it transitions into the cloud and into our homes.[16] In particular, what practical challenges will cloud robotics face should it transition into a mainstream consumer industry and attempt to adopt contemporary variations of the Fair Information Practices? Why should the cloud robotics industry begin to understand these challenges now? How can roboticists open a dialog with privacy advocates, policymakers, and regulators on how to best maintain both innovation and consumer privacy expectations as robots begin to connect to the Internet? These questions form the basis of this Paper.

Section I introduces the concept of cloud robotics. This Section examines how, historically, robots have been limited by 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."[17] Section II provides a brief history of the FIPPs, while specifically

[15] *See, e.g.*, Ryan Calo, *Robots and Privacy*, in ROBOT ETHICS : THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS 187–198 (eds. Patrick Lin, Keith Abney & George A. Bekey) (2012) (outlining "the effects of robots on privacy into three categories—direct surveillance, increased access, and social meaning"); Ryan Calo, *They're Watching. How Can That Be A Good Thing?*, STANFORD ALUMNI, Jan./Feb. 2014 (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); Denning et. al. *supra* note 12 (analyzing three household robots for security and privacy vulnerabilities, "identify[ing] key lessons and challenges for securing future household robots" and "propos[ing] a set of design questions aimed at facilitating the future development of household robots that are secure and preserve their users' privacy").

[16] *See* Denning et. al. *supra* note 12, at 105 ("[T]here is currently a marked void in the consideration of the security and privacy risks associated with household robots."); *but see* Aneta Podsiadła, *What Robotics Can Learn from the Contemporary Problems of Information Technology Sector: Privacy by Design as a Product Safety Standards-Compliance and Enforcement*, *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 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 manufactures who fail to implement).

[17] P.H., *Artificial Intelligence Networks: We, Robots*, BABBAGE, Jan. 21, 2014, *available at* http://www.economist.com/blogs/babbage/2014/01/artificial-intelligence-networks.

examining two contemporary FIPPs frameworks developed by the Federal Trade Commission ("FTC") and the Obama Administration. Section III examines the unique challenges facing cloud robotics should it apply contemporary variations of the FIPPs. This Section limits its examination to cloud-enabled robots functioning 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 privacy and robotics communities.

I. CLOUD ROBOTICS & TOMORROW'S DOMESTIC ROBOTS

The concept of "robots" is hard to clearly delineate, but all robots are multi-function devices with the capability to sense the environment and act on its environment using movement.[18] "Intelligence" is the connection between sensing and acting, and it can be implemented in many ways. The simplest forms of intelligence could be a set of fixed computational rules (e.g., if-then statements) or mathematical formulas (e.g., linear feedback controllers). However, the intelligence needed to perform tasks expected of humans in unstructured environments such as the home must be much more complex. Intelligent robots in domestic environments should incorporate 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. As a result, modern general-purpose domestic robots are implemented as very large software systems, composed of

[18] *See, e.g.*, Bill Gates, *A Robot in Every Home*, SCIENTIFIC AMERICAN, 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."); Denning et. al, *supra* note 12, at 105 (defining "robot" for their study as "a physical systems with sensors actuators and mobility"); NEIL M. RICHARDS & WILLIAM D. SMART, HOW SHOULD THE LAW THINK ABOUT ROBOTS? 5 (2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2263363 (preliminary draft) (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.").

multiple modules running sophisticated algorithms, each of which require significant computational power.[19]

In cloud robotics, the software for implementing intelligent and/or autonomous behavior is partially or fully shifted to "the cloud"—remote computers communicating to the robot via the Internet. This moves the locus of "intelligence" from onboard the robot to a remote service. There are several advantages to such an architecture. First, robots can be made cheaper, because costs are reduced by eliminating the need for powerful onboard computers. Moreover, robots may be able to use cheaper sensor and actuator hardware, because the use of more powerful computing resources can sometimes compensate for the inaccuracies of the hardware. Fewer onboard computers also means lowering energy usage and prolonging battery life, which is one of the greatest practical limitations to consumer robotics.

Second, the cloud may provide improved functionality. Computationally complex tasks, such as object recognition, sensor fusion, and planning, can be solved using "brute force" on the cloud with many parallel computers. Moreover, the cloud has easier access to common information from the web and from other robots, which could improve performance in tasks like object recognition due to the use of extensive existing databases on the web (e.g., Google Image Search, Flickr) or the prior experience of other robots. This results in vastly increased object datum points, providing increased opportunities for robots to interact with objects and their environments. Robots may also need to "call for help" when in a jam, and human tele-operators may be able to help, similar to Amazon's Mechanical Turk service.[20]

[19] *See, e.g.*, *Why ROS?: Core Components*, ROS.ORG, http://www.ros.org/core-components/ (last visited March 12, 2014) (identifying some of the core parts of the robot operating system, ROS).

[20] *See Amazon Web Services Amazon Mechanical Turk (Beta)*, AMAZON.COM, http://aws.amazon.com/mturk/ (last visited March 12, 2014).

Finally, it is easier for a service provider to debug and update software on the cloud than in the consumer's home. Software updates become transparent, because a cloud service can be updated without access to the physical robot. Likewise, human technicians can perform remote debugging without physical access to the robot.

Current cloud robots tend to use the cloud only for certain functions, such as object recognition, or to store large 3D maps. 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"[21] that transmits sensor data to the service and receives instructions from the service. 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. Current cloud robots perform some limited perceptual processing to avoid transmitting huge amounts of sensor data (e.g., multiple video streams) to the cloud,[22] but in the future it is likely that these bandwidth limitations will become less restrictive. In the fully cloud-enabled case, the cloud service will see everything the robot sees.

As cloud robotics concepts continue to advance, entities are beginning to recognize the potential 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."[23] The goal of RoboEarth is "to use the Internet to create a giant open source network database that can be accessed and continually

[21] 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, Brian Gerkeyy, Ken Conleyy, Josh Fausty, Tully Footey, Jeremy Leibsz, Eric Bergery, Rob Wheelery & Andrew Ng, *ROS: an Open-source Robot Operating System*, in ICRA WORKSHOP ON OPEN SOURCE SOFTWARE (2009), *available at* http://pub1.willowgarage.com/~konolige/cs225B/docs/quigley-icra2009-ros.pdf (proposing a "'thin' ideology" for a cloud-based robot operating system, ROS, that "encourage[s] all driver and algorithm development to occur in standalone libraries that have no dependencies on ROS").

[22] *See, e.g.*, Markus Waibel & Gajan Mohanarajah, *Mapping in the Cloud*, ROBOHUB, Dec. 23, 2013, www.robohub.org/mapping-in-the-cloud/.

[23] *See* Waibel et. al., *supra* note 8, at 71.

updated by robots around the world," thus allowing robots to enter "unstructured environments" and operate in the real world.[24] 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.[25] 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."[26] Google, as well, has set its sights on a robot marketplace, and has recently "acquired seven technology companies in an effort to create a new generation of robots."[27] Google has already provided benefits for cloud-enabled robots, as researchers have used Google products, such as Google Glass, for object recognition to implement robot grasping tasks.[28]

Overall, a number of noteworthy characteristics emerge after reviewing current cloud robotics concepts. First, given the complexity of allowing robots to operate in an unstructured environment, the "datafication" and collection of a robot's environment will be expansive and necessary.[29] This will include not only the specific mapping of buildings and rooms, but also particular data on objects within that environment, including data that will help determine what the object is and information on where the object is located. Second, due to this unstructured environment, unforeseen obstacles may make the data necessary to complete a specific task unknown at the time in which the data are collected.[30] Finally, the goal of pooling, sharing, and

[24] See *Motivation*, ROBOEARTH, http://roboearth.org/motivation (last visited March 5, 2014).
[25] *See* Waibel et. al., *supra* note 8, at 70.
[26] Mohanarajah Gajamohan, *RoboEarth 4th Year Demonstration*, ROBOEARTH BLOG, Jan. 13, 2014, *available at* http://roboearth.org/archives/2458.
[27] John Markoff, *Google Puts Money on Robots, Using the Man Behind Android*, N.Y. TIMES, Dec. 4, 2013, at A1
[28] *See* Ben Kehoe, Akihiro Matsukawa, Sal Candido, James Kuffner & Ken Goldberg, *Cloud-Based Robot Grasping with the Google Object Recognition Engine, in* IEEE INTERNATIONAL CONFERENCE ON ROBOTICS AND AUTOMATION 1 (2013), *available at* http://queue.ieor.berkeley.edu/~goldberg/pubs/Grasping-with-Google-Goggles-icra-2013.pdf.
[29] "Datafication," coined by Viktor Mayer-Schonberger and Kenneth Cukier, is the act of transforming something into "a quantified format so it can be tabulated and analyzed." VIKTOR MAYER-SCHONBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 76 (2013)
[30] Hani Hagras & Tarek Sobh, *Intelligent Learning and Control of Autonomous Robotic Agents Operating in Unstructured Environments*, 145 INFO. SCIENCE 1, 2 (2002) ("[I]t is not possible to have exact and complete prior

reusing data as a method to allow 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.[31] It is this widespread and intimate collection of data, this appropriation of data for unanticipated purposes, and this 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 Fair Information Practice Principles have been described as the "gold standard" for protecting personal information.[32] 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."[33] The 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."[34] At their inception, the FIPPs "reflected a wide consensus about the need for broad standards to

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.").

[31] P.H., *supra* note 17 (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.").

[32] *See Fair Information Practice Principles (FIPPs) Privacy*, BERKELEY SECURITY, https://security.berkeley.edu/fipps (last visited March 5, 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.").

[33] ROBERT GELLMAN, FAIR INFORMATION PRACTICES: A BASIC HISTORY 1 (2013).

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

facilitate both individual privacy and the promise of information flows in an increasingly technology-dependent, global society."[35]

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.[36] 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."[37] In order to diminish such practices, the Report called for the enactment of a Federal "Code of Fair Information Practices,"[38] which would result in the core cannons of the FIPPs.

The FIPPs were articulated in perhaps their most influential form in 1980 by the Organization for Economic Co-operation and Development (OECD). Finding at the time that there was a "danger that disparities in national legislations could hamper the free flow of personal data across frontiers," which "could cause serious disruption in important sectors of the economy,"[39] 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

[35] Fred H. Cate, *The Failure of Fair Information Practice Principles in* CONSUMER PROTECTION IN THE AGE OF THE 'INTERNET ECONOMY, 341, 341(ed. Geraint Howells) (2006).

[36] DEPARTMENT OF HEALTH, EDUCATION AND WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS 1 (1973). Gellman notes that, at the same time of the Health, Education and Welfare Report, a "Committee on Privacy" was held in Great Britain, which proposed many of the same principles. GELLMAN, *supra* note 33, at 3. 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]." GELLMAN, *supra* note 33, at 4.

[37] DEPARTMENT OF HEALTH, EDUCATION AND WELFARE, *supra* note 36, at xx.

[38] These principles were as follows: "There must be no personal data record keeping systems whose very existence is secret"; "There must be a way for an individual to find out what information about him is in a record and how it is used"; "There 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 "There must be a way for an individual to correct or amend a record of identifiable information about him." *Id.*

[39] *Preface: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD.ORG, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last visited March 5, 2014).

interruptions in international flows of data."[40] 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."[41] These principles, reaffirmed in 2013,[42] include: Collection Limitation; Data Quality; Purpose Specification; Use Limitation; Security Safeguards; Openness; Individual Participation; and Accountability.[43]

The OECD Guidelines, however, are not the only articulated set of FIPPs principles.[44] To this end, "the FIPPs" are not a single, standard set of rules, but are generally discussed as abstract practices that have evolved into "different formulations coming from different countries and different sources over the decades."[45] The terminology, emphasis, and articulation of these formulations can vary significantly, but a few commonalities exist across the resulting frameworks and regulations: (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.[46] The procedural

[40] *Id.*

[41] *Id.*

[42] *See* ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, THE OECD PRIVACY FRAMEWORK (2013).

[43] *Id.* at 13-15. In addition to reaffirming the traditional principles, the 2013 revisions aimed "to assess the Guidelines in light of 'changing technologies, markets and user behavior, and the growing importance of digital identities.'" The new concepts introduced in the revised Guidelines include "National 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," "Privacy management programmes," which serve as the core operational mechanism through which organisations implement privacy protection," and "Data 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.*

[44] Both the White House Consumer Privacy Bill of Rights and the Federal Trade Commission Privacy Framework, discussed below, have cite to the OECD guidelines as guiding the creation of these more contemporary frameworks.

[45] GELLMAN, *supra* note 33, at 1; *but see* Cate, *supra* note 35 at 341 (arguing that the FIPPs integration into US and European law has caused the FIPPs to be "reduced to narrow, legalistic principles.").

[46] 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* Part 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 CAL. L. REV. (forthcoming 2014) (explaining different US approaches to determining personally indefinable information, including the "specific-types" approach).

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."[47] 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."[48]

With the advent of the Internet, and the tremendous increase in consumer data being collected and used by companies, national and international regulators began to increasingly focus on FIPPs frameworks, such as the OECD Guidelines, as the foundation for laws protecting personal information. Unlike other international regulations,[49] no omnibus U.S. law regulates the use or collection of personal consumer data.[50] Recognizing this void, current federal policymakers have started crafting updated privacy "best practices," based largely on the FIPPs and reflect current commercial norms. These "contemporary" FIPPs frameworks attempt to balance adequate privacy practices and flexibility for companies in such a data-driven, Internet-dependent society. Recent approaches have adopted practices that focus on the "context of the transaction"[51] or the "sensitivity" of the data[52] as methods for providing more flexible standards. In addition to heralding these frameworks as providing consumer privacy best practices, many

[47] FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS 48 n.28 (1998).
[48] *Id.*
[49] *See, e.g.*, Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 2(a), 1995 O.J. (C 93).
[50] Federal statutes, however, have been enacted that regulate data privacy and security for a small subset of industry sectors and for particular types of data. See Kenneth A. Bamberger & Deirdre K. Milligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 255-56 (2011). The Federal Trade Commission, 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.*, In re of Facebook, Inc., Decision and Order, File No. 092 3184 (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).
[51] *See e.g.*, *infra* Part II.B.4.
[52] *See e.g.*, *infra* Part II.C.1.

policymakers have advocated for legislation that would require companies to implement these baseline practices.[53]

Two recent variations of such contemporary FIPPs frameworks offer a foundation on which to examine how cloud robotics may interact with 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 Federal Trade Commission's Privacy Framework in its report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*. As cloud robotics becomes more feasible and cloud-enabled domestic robots begin to garner discussion as a plausible architecture for consumer robots, 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's Privacy Framework can assist in articulating challenges and developing discussion.

B. The Consumer Privacy Bill of Rights

In February 2012, the White House and the Department of Commerce observed that, despite the fact that the current consumer data privacy framework is strong, it "lacks 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."[54] It is in this context that the Obama Administration issued a new variation of the FIPPs in its report, *A Framework for Protecting*

[53] See FTC PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 12-13 (2012) [hereinafter 2012 FTC PRIVACY REPORT] ("[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 13.

[54] *Id.* at i.

Privacy and Promoting Innovation in the Global Digital Economy. The Report's privacy framework, the "Consumer Privacy Bill of Rights," is described as "a blueprint for privacy in the information age" that "give[s] consumers clear guidance on what they should expect from those who handle their personal information, and set[s] expectations for companies that use personal data."[55]

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."[56] 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."[57] To "carry the 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."[58] The Consumer Privacy Bill of Rights consists of seven principles: Individual Control, Transparency, Respect for Context, Security, Access and Accuracy, Focused Collection, and Accountability.

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 [are] linkable to a specific individual. Personal data may include data that [are] linked to a specific computer or other

[55] *Id.* at intro (Statement of President Obama).
[56] *Id.* at 1.
[57] *Id.* at 9.
[58] *Id*.

device."[59] 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."[60]

2. Individual Control

First, the Consumer Privacy Bill of Rights lays out a principle of Individual Control. It states that "[c]onsumers have a right to exercise control over what personal data companies collect from them and how they use it."[61] This principle contains two "dimensions," one placing obligations on companies and another defining the responsibilities of consumers.[62]

The first dimension of the principle says that "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."[63] 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."[64] 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."[65]

[59] *Id.* at 10 ("For example, an identifier on a smartphone or family computer that is used to build a usage profile is personal data. This definition provides the flexibility that is necessary to capture the many kinds of data about consumers that commercial entities collect, use, and disclose.").
[60] *Id.*
[61] *Id.* at 47.
[62] *Id.* at 11.
[63] *Id.* For example, in cases where a company has access to Internet usage histories which can build 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.*
[64] *Id.*
[65] *Id.*

In addition, the Individual Control principle has a second dimension regarding "consumer responsibility." 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."[66] The Administration stresses that "[c]onsumers should take responsibility for those decisions, just as companies that participate in and benefit from this sharing should provide usable tools and clear explanations to enable consumers to make meaningful choices."[67]

Finally, Individual Control contains a "right to withdraw consent to use personal data that the company controls."[68] According to the Administration, "[c]ompanies should provide means of withdrawing consent that are on equal footing with ways they obtain consent."[69] 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."[70] Further, "the obligation to respect a consumer's withdrawal of consent only extends to data that the company has under its control."[71]

3. Transparency

The Transparency principle states that "[c]onsumers have a right to easily understandable and accessible information about privacy and security practices," and "companies should provide clear descriptions of what personal data they collect, why they need the data, how they will use

[66] *Id.* at 13.
[67] *Id.*
[68] *Id.*
[69] *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.").
[70] *Id.* at 14.
[71] *Id.*

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."[72] 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."[73] 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."[74] The form of these notices should be "easy to read on the devices that consumers actually use to access their services."[75] 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." [76]

4. Respect for Context

A cornerstone of the Consumer Privacy Bill of Rights, the Respect for Context principle states that "[c]onsumers 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."[77] Therefore, "[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

[72] *Id.*

[73] *Id.*

[74] *Id.* at 14.

[75] *Id*. 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.*

[76] *Id*. (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").

[77] *Id.* at 47. Respect for Context, in part, derives from the OECD Framework's Purpose Specification and Use Limitation principles. *Id.* at 16.

otherwise."[78] 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," the principle calls for the companies to provide heightened measures of Transparency and Individual Choice.[79]

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 disclose data, [but] also recognizes that this relationship may change over time in ways not foreseeable at the time of collection."[80] 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."[81] 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, understandings, and level of sophistication.[82] 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."[83]

[78] *Id.* at 47.
[79] *Id.* at 47-48.
[80] *Id.*
[81] *Id.*
[82] *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.
[83] *Id.* at 16.

5. Security

The Security principle states that "[c]onsumers have a right to secure and responsible handling of personal data," which means that "[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."[84] The Administration elaborates that "[t]he security precautions that are appropriate for a given company will depend on its lines of business, the kinds of personal data it collects, the likelihood of harm to consumers, and many other factors."[85]

6. Access and Accuracy

The Access and Accuracy principle states that "[c]onsumers 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 [are] inaccurate."[86] According to this principle, companies "should use reasonable measures to ensure they maintain accurate personal data," and "should 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."[87] Further, "[i]n determining what measures they may use to maintain 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

[84] *Id.* at 48.
[85] *Id.* at 19.
[86] *Id.* at 48.
[87] *Id.*

expose consumers to financial, physical, or other material harm."[88] These factors "help to determine what kinds of access and correction facilities may be reasonable in a given context."[89]

7. Focused Collection

The Focused Collection principle states that "Consumers have a right to reasonable limits on the personal data that companies collect and retain."[90] This means that "[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 de-identify personal data once they no longer need it, unless they are under a legal obligation to do otherwise."[91] This requires companies to "engage in considered decisions about the kinds of data they need to collect to accomplish specific purposes."[92]

8. Accountability

The Accountability principle states that "[c]onsumers 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," and lays out the ways in which "[c]ompanies should be accountable to enforcement authorities and consumers."[93] 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."[94] Among other things, this means that companies "should hold employees responsible for adhering to these principles," and should train them "as appropriate to handle personal data consistently with these principles and

[88] *Id.*
[89] *Id.* at 20.
[90] *Id.* at 48.
[91] *Id.*
[92] *Id.* at 21. 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.*
[93] *Id.* at 48.
[94] *Id.* at 22.

regularly evaluate their performance in this regard."[95] 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 "size, complexity, and nature of a company's business, as well as the sensitivity of the data involved."[96]

C. The 2012 Federal Trade Commission Privacy Framework

In late 2009, then-current 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."[97] Recognizing the "increase[ed] advances in technology" that had allowed for "rapid data collection and sharing that is often invisible to consumers," the Commission sought to develop a framework that businesses could utilize to reduce the burden on consumers to protect their own privacy.[98] In 2012, following a series of roundtable discussions and a period of public comment after the release of a preliminary report, the Commission issued *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers* (the "FTC Report").[99] The FTC Report was "intended to articulate best practices for companies that collect and use consumer data,"[100] and to assist companies in developing and maintaining "processes and systems to operationalize privacy and data security practices within their business"[101]

[95] *Id.* at 48.
[96] *Id.*
[97] Introductory Remarks of Chairman Jon Leibowitz, FTC Privacy Roundtable, Dec. 7, 2009, at 1 (citing to the publication of *The Right to Privacy* in the Harvard Law Review and the surveillance abuses of the Nixon Administration as other previous watershed moments in privacy), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/introductory-remarks-ftc-privacy-roundtable/091207privacyremarks.pdf.
[98] Press Release, FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers, Dec. 1, 2010, *available at* http://www.ftc.gov/news-events/press-releases/2010/12/ftc-staff-issues-privacy-report-offers-framework-consumers.
[99] 2012 FTC PRIVACY REPORT, *supra* note 53.
[100] *Id.* at iii.
[101] *Id.* at 1.

Central to the FTC Report is the FTC Privacy Framework, consisting of principles for companies to implement in order to achieve best consumer privacy practices.[102] The FTC Report supplements the FTC Privacy Framework by providing in-depth commentary on interpretations of the Framework's final and baseline principles, and suggesting practical mechanisms to implement the Framework. The FTC Privacy 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.

1. Scope

According to the FTC Framework,

> The 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 nonsensitive data from fewer than 5,000 consumers per year and does not share the data with third parties.[103]

The scope in which the Framework applies is intentionally broad, and intended 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.[104] Key to the FTC Privacy Framework's scope is that consumer data be "reasonably linked" to a specific consumer, computer, or other device. The Framework articulates that information will not be considered "reasonably linked" if three criteria are met: first, "the company must take reasonable measures to ensure that the data [are] de-identified"[105]; second, "a company must publicly commit to

[102] *Id.* at vii-viii.

[103] *Id.* at 22.

[104] *See id.* at 17-18.The FTC Report does note that some commercial sectors have statutory obligations already imposed upon them concerning proper data practices and notes 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.

[105] *Id.* at 21.The FTC further specifies this requirement, stating that this 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.* at 21 (internal footnotes omitted).

maintain and use the data in a de-identified fashion, and not to attempt to re-identify the data"; and third, "if a company makes such de-identified data available to other companies – whether service providers or other third parties – it should contractually prohibit such entities from attempting to re-identify the data."[106]

The FTC Framework additionally provides an exception for companies that collect nonsensitive data, for less than 5,000 consumers per year, and do not share that data with a third party. The FTC Framework refrains from providing a set definition of what constitutes "sensitive" data, stating that 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."[107] However the FTC Report does find that at a minimum, nonsensitive data includes "data about children, financial and health information, Social Security numbers, and certain geolocation data."[108]

2. <u>Privacy By Design</u>

The first major baseline principle under the FTC Privacy Framework is "Privacy by Design," which states that "[c]ompanies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services."[109] The concept of Privacy by Design calls on companies to "build in" both substantive and procedural privacy safeguards to everyday business operations.

The Privacy by Design procedural principle states, "[c]ompanies should maintain comprehensive data management procedures throughout the life cycle of their products and services."[110] The FTC Report suggests that this principle can be achieved by implementing practices, such as accountability mechanisms, to ensure that privacy issues are addressed

[106] *Id.*
[107] *Id.* at 60.
[108] *Id.* at 42 n.214.
[109] *Id.* at 22.
[110] *Id.* at 32.

throughout an organization and its products.[111] These mechanisms are intended to ensure the proper implementation of the Privacy by Design substantive principles specifically and the FTC Privacy Framework generally.

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 and disposal practices, and data accuracy."[112]

As the FTC Report notes, "[i]t is well settled that companies must provide reasonable security for consumer data."[113] 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."[114]

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."[115] 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."[116] Similar to the White House Consumer Bill of Rights Framework, discussed above,[117] limiting data collection to the context of the transaction "is

[111] *See id.* at 30–32.
[112] *Id.* at 23.
[113] *Id.* at 24.
[114] *Id.* at 25.
[115] *Id.* at 30.
[116] *Id.* For a more in-depth discussion on consumer choice, see *infra* Part II.C.3.
[117] *See supra* at Part II.B.7.

intended to help companies assess whether their data collection is consistent with what a consumer might expect."[118]

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. The FTC Report states that "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."[119] A reasonable period under the FTC Privacy Framework "can be flexible and scaled according to the type of relationship and use of the data."[120] 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.[121]

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."[122] However, recognizing the need to create flexibility for companies, the Report notes that "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."[123]

3. Simplified Consumer Choice

The Simplified Consumer Choice baseline principle states that "[c]ompanies should simplify consumer choice."[124] Because of the "dramatic increase in the breadth of consumer

[118] 2012 FTC PRIVACY REPORT, *supra* note 53, at 27.
[119] *Id.* at 27.
[120] *Id.*
[121] *Id.*
[122] *Id.* at 29 (referencing the 2010 preliminary staff report that preceded the final Report).
[123] *Id.* at 30 ("[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 . . .").
[124] *Id.* at 35.

data," the lack of legal requirements on companies to provide consumer choice, and the inadequacy of privacy policies to effectively communicate consumer choices, the Simplified Consumer Choice principle intends to recommend methods of choice that would be more effective and less burdensome on consumers.[125] The Simplified Consumer Choice is broken down into two parts (1) when consumer choice may be unnecessary, and (2) what constitutes an "appropriate method" of consumer choice when such choice is necessary.

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."[126] Similar to the Consumer Privacy Bill of Rights, the FTC Framework states that the "context of the transaction" standard generally depend on reasonable consumer expectations, but focuses on more objective factors related to the consumer's relationship with a business.[127] The FTC Report expands on its discussion of its context standard, stating that product or service fulfilment, 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."[128]

Second, in the event that choice would be appropriate, the FTC Framework's Simplified Consumer Choice principle states:

> companies 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

[125] *Id.*
[126] *Id.* at 48.
[127] *Id.* at 38.(recognizing that some practices produced "reduced benefits for providing choices to consumers about their data" because "consent can be inferred" or "public policy makes choice unnecessary").
[128] *Id.* at 38-39. 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, 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.

> different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes.[129]

In regards 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."[130] Again, relying on the idea of context, the FTC Report does not define an ironclad point in 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.[131]

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.[132] At the same time, flexibility is needed in order to avoid "choice fatigue."[133] As the FTC Report states, "Consumers' privacy interests ought not to be put at risk in . . . one-sided transactions."[134] Overall, companies are tasked with providing consumer 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,"[135] is appropriate when information is used (1) "in a materially different manner than claimed when the data was

[129] *Id.* at 60.
[130] *Id.* at 49–50.
[131] *Id.* at 50.
[132] *Id.* at 51. "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.
[133] *Id.* at 49.
[134] *Id.* at 52.
[135] *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.").

collected"; or (2) to "collect[] sensitive data for certain purposes."[136] The FTC Report explains that use of consumer data in a "materially different manner" may be determined on a "case-by-case basis."[137] The FTC Report also states that affirmative expressed consent should be obtained before collecting sensitive data.[138]

4. Transparency

Finally, the Transparency principle states, "[c]ompanies should increase the transparency of their data practices."[139] Specifically the Transparency principle includes a Privacy Notice principle, and an Access principle.[140] Under the Privacy Notice 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."[141] 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."[142] However, the FTC Report notes that such standardization can be difficult when technologies vary in their hardware specifications, such as mobile devices that contain smaller screens.[143]

Under the Access principle, the FTC Framework states that "[c]ompanies should provide reasonable access to the consumer data they maintain; the extent of access should be

[136] *Id.* at 60.

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

[138] *See id.* at 58–60.

[139] *Id.* at 60.

[140] The FTC Framework's Transparency principle also includes a final principle, the Consumer Education Principle, which states that "[a]ll stakeholders should expand their efforts to educate consumers about commercial data privacy practices." Because this Principle goes beyond the purposes of this Paper, it is not discussed.

[141] *Id.* at 64.

[142] Id. at 62.

[143] *See id.* at 63–64.

proportionate to the sensitivity of the data and the nature of its use."[144] 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 benefits.[145] 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 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."[146]

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 contemporary FIPPs approaches 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. As cloud robotics becomes more of a reality, it is important to start understanding where, and to what extent, current technological data collection and use practices differ from current concepts of cloud robotics. With this understanding, roboticists may be empowered to constructively contribute to the debate over how to properly regulate data in the up-and-coming consumer robot marketplace. Technologists and roboticists alike can also begin to research the development of privacy-enhancing technologies. Throughout this evaluation, this Section recognizes some practical challenges cloud robotics may face in applying contemporary FIPPs frameworks.

[144] *Id.* at 71

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

[146] *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.").

Where appropriate, similarities and distinctions from current technologies are presented, and possible alternative solutions are raised.

This Section begins by determining how to properly characterize data collected by a cloud-enabled domestic robot, including the issue of whether to classify data related to objects found within a domestic environment as "sensitive." 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 in determining what 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. 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. Finally, the principles of Transparency, Security, Access and Accuracy, and Accountability 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 concentrate discussion, this Section limits the scope in which it examines cloud robotics. First, when necessary, this Section considers only the privacy implications that arise directly between the consumer-facing cloud robotics company and the user.[147] Second, this Section is limited to the privacy issues that might

[147] This assumption is made 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. As cloud robotics continues to develop, it would be wise to consider the privacy implications that may arise from these additional issues.

arise from cloud enabled-robots “designed and priced for use within a home or other domestic environment.”[148]

A. The “Sensitivity” of Data Collected by Cloud-Enabled Robots In a Domestic Environment

Before cloud-enabled robots enter the home, companies will need to fully understand whether the information their robots will collect is “personally identifiable,” and more importantly, how “sensitive” that data will be. Generally speaking, contemporary FIPPs frameworks apply to data that is “personally identifiable” to a person or device.[149] Current concepts in cloud robotics rely on data that is likely to be considered personally identifiable. The data RoboEarth collects, uses, and retains, for instance, is highly identifiable. The RoboEarth database’s “Environment” table 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.[150] Object data collected and stored, too, contain precise tags that include the location of an object, as well as the time an object was detected.[151] Thus, the geolocation metadata tags captured, utilized, and stored by a cloud-enabled robot will likely cause much of that data to be linkable to the robot and possibly the user.

A more challenging issue will be determining data sensitivity. The term “sensitive,” as used by contemporary frameworks, is intentionally subjective to provide flexibility. The FTC Privacy Framework, for instance, stated that the determination is one that is “in the eye of the

[148] Denning et. al, *supra* note 12, at 106.
[149] *See supra* Part II.B.1; *supra* note Part II.C.1.
[150] BJÖRN SCHIEßLE, KAI HÄUSSERMANN, & OLIVER ZWEIGLE, COMPLETE SPECIFICATION OF THE ROBOEARTH PLATFORM 13 (2010).
[151] *See,* Waibel et. al., *supra* note 8, at 73–74 (explaining how objects, environments, and action recipes are stored).

beholder."[152] However, the term is one of significant importance for companies attempting to adhere to contemporary FIPPs frameworks, as the "sensitivity" of personally identifiable information, in many cases, determines the rigidity of the framework's practices.[153] Pose the question of what is "sensitive" data to a world where cloud-enabled robots are operating within the home, and numerous questions start to arise.

An individual's home, and the items within it, have been traditionally afforded heightened privacy protections. Regardless of the items that may be contained there, the simple act of "being in the home" has been enough to induce these heightened privacy protections. Constitutionally, we have seen an individual's "residential privacy" interest outweigh another's First Amendment right to freedom of speech.[154] Government entities are required to obtain a warrant for searches within an individual's home because of the heighten expectation of privacy the location provides, regardless of "the quality or quantity of information obtained."[155] Because of these significant privacy protections, would cloud-enable robots collecting information inside the home, regardless of what that information may be, garner a classification of "sensitive" data and thus be subject to more restrictive practices? Does the sensitive nature of an individual's geolocation extend to the geolocation data of objects residing in a user's home? For example, if a cloud-enabled robot collects and stores data related to a particular cup known to be sitting on a user's kitchen table, would that data be labeled as "sensitive?" Companies distributing cloud-

[152] *See* 2012 FTC PRIVACY REPORT, *supra* note 53, at 60.

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

[154] *See, e.g.,* FCC v. Pacifica Foundation, 438 U.S. 726, 748 (1978) (opining that "the individual's right to be left alone plainly outweighs the First Amendment rights of an intruder"); Frisby v. Schultz, 487 U.S. 474, 486 (holding that targeted residential picketing "inherently and offensively intrudes on residential privacy," and such activities can have a "devastating effect" on the quite enjoyment of the home).

[155] Kyllo v. United States, 533 U.S. 27, 37 (2001); *see also* Florida v. Jardines, 133 S. Ct. 1409 (2013) (reaffirming that at 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'" (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

enabled domestic robots, looking to limit unnecessary practices that could get in the way of a robot's functionality, would be inclined to argue that such benign data is much less sensitive than the location of the actual user, if sensitive at all. Consumer expectation, however, may reflect a different view.

Certain methods and practices, however, could be utilized in order to de-identity data, thus preventing application of the FIPPs in the first place. Some variations of the FIPPs, the FTC Framework in particular, recognize that information that is "de-identified" will not be considered reasonably linked to the user or device, so long as the entity collecting and using the information agrees to not re-identify the data.[156] Numerous privacy-enhancing technologies have been created to help de-identify data,[157] and de-identification methods that would allow for cloud-enabled robots to still function effectively could greatly offset any hindrance that other FIPPs principles might have on cloud-enabled robots. However, in practice, these privacy enhancements may offset the functional advantages of keeping data personally identifiable.[158]

B. The Context of a Cloud-Enabled Robot Transaction: Data Collection, Use, and Retention Limitations

In addition to determining the rigidity of principles based upon the sensitivity of data, contemporary FIPPs frameworks determine the rigidity of principles based upon the "context" in which a user discloses his or her data. Under this context-centric approach, the collection,[159]

[156] *See supra* Part II.B.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.*

[157] *See e.g.*, ROBERT TEMPLEMAN, MOHAMMED KORAYEM, DAVID CRANDALL & APU KAPADIA, PLACEAVOIDER: STEERING FIRST-PERSON CAMERAS AWAY FROM SENSITIVE SPACES 1 (2014) (presented at the Internet Society's 2014 Network and Distributed System Security Symposium) (demonstrating the "PlaceAvoider" technique for first-person cameras, which "blacklists" sensitive spaces by "recognize[ing] images captured in these spaces and flags them for review before the images are made available to applications").

[158] *See* Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1200 (finding that anonymous information in the context of autonomous vehicles, "should be sufficient for such uses as transportation planning, traffic management and the like," but "[t]he challenge will be to maintain the anonymity of this information, which often gains value when linked to an identifiable person.").

[159] *See e.g.*, *supra* Part II.B.7 (stating that companies should collection "only as much personal data as they need to accomplish purposes specified under the Respect for Context principle"); *supra* Part II.C.2 (stating that data

use,[160] and retention[161] limitations of data all hinge on the context in which data are disclosed by the user, and the relationship the user has with the entity collecting, using, or retaining the data. Data practices that are considered to be within the context of a particular transaction may be exempt, in certain circumstances, from providing meaningful choice mechanisms for consumers.[162]

"Context," like much of the terminology in contemporary FIPPs 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."[163] From a contemporary FIPPs perspective, 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, just to name a few.[164] 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.[165] In general, the context-centric approach to 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

collection should be limited "to that which is consistent with the context of a particular transaction or the consumer's relationship with the business").

[160] *See e.g.*, *supra* Part II.B.4 (stating that consumer have a right to expect companies to use their data "in ways that are consistent with the context in which consumers provide the data."); *supra* Part II.C.2 (stating that companies do not need to provide choices when "using consumer data for practices that are consistent with the context of the transaction").

[161] *See e.g.*, *supra* Part II.B. 7 (stating that companies should dispose of or de-identify data "once they no longer need it"); *supra* Part II.C.2 (stating that companies should dispose of data "once the data has outlived the legitimate purpose for which it was collected").

[162] *See e.g.*, WHITE HOUSE PRIVACY REPORT, *supra* note 13 at 17 (explaining how retailers may need to communicate consumers' name and address to fulfill shipping requests, which "is obvious for the context of the consumer-retailed relationship" and thus "do[es] not need to provide prominent notice" and retailers may infer consent)

[163] WORLD ECONOMIC FORUM, UNLOCKING THE VALUE OF PERSONAL DATA: FROM COLLECTION TO USAGE 11(2013).

[164] *See e.g.*, *supra* Part II.B.4.

[165] *See supra* note 128 & accompanying text.

companies themselves explain the roles of personal data in delivering them, research on consumer attitudes, and feedback from consumers."[166]

Even under this more flexible standard, however, challenges exist for companies providing 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 going to be useful.[167] 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."[168] 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."[169] 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.[170] 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.

Cloud robotics, in a sense, relies on a broader, more open-ended purpose for the data it collects and uses. The architecture of 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. The data needed for a robot to grasp a particular cup in your home, for

[166] WHITE HOUSE PRIVACY REPORT, *supra* note 13, at 16.

[167] *See* Raymond Reiter, *On Closed World Data Bases, in* LOGIC AND DATA BASES 119–140 (eds. Hervé Gallaire & Jack Minker) (1977)

[168] NICO HUBEL, GAJMOHAN MOHANARAJAH, RENÉ VAN DE MOLENGRAFT, MARKUS WAIBEL & RAFFAELLO D'ANDREA, LEARNING AND ADAPTATION IN DYNAMIC SYSTEMS: A LITERATURE SURVEY 4 (2010)

[169] *Id.*

[170] See Ryan Calo, *Open Robotics*, 70 MD. L. REV. 101, 114 (2011).

instance, may later become part of a more complex task for a robot, such as serving a drink to a particular user.[171] 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 in which the user agreed to originally disclose the information.

Such broad, open-ended purposes may be unfamiliar and difficult for users to comprehend, making the context of any such task difficult to delineate. What may result is a disconnect between what users expect the context of a particular cloud-enabled robot transaction to be, and what cloud robotics strives to achieve. This disconnect makes setting proper data collection, use, and retention limits difficult. For instance, assume a user tasks a cloud-enabled robot to serve the user a drink. A consumer-centric interpretation may expect that the data collected about the cup, or any data collected in order to complete the task, is limited to the context of that particular drink-serving task. The company's interpretation, on the other hand, would likely be broader, possibly extending the use to other tasks like dish-washing, and even sharing the data with other consumers' robots to aid in future drink-serving tasks. For these reasons, determining the appropriate balance between meeting consumer expectations and enabling product fulfillment will prove to be critical.

These difficulties may lead to inconsistent data practices among companies, which could signal an unjustifiable risk to consumer data and their privacy. Such risks have been found in similar new technologies, including Internet-connected cars. 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

[171] *See e.g.*, Waibel et. al., *supra* note 8, at 74, Fig.5 (explaining how the "GraspBottle" task may become part of the "ServeaDrink" function task).

developers] retain vehicle-specific or personally identifiable location data."[172] 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."[173] 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 contemporary FIPPs frameworks,[174] will prove difficult with "context" as the guide.

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 the difficult-to-define "context." Privacy concerns that result from the vast collection of data[175] may be magnified due to the sheer volume of data that must be collected in order for cloud robotics to function. It will be important to consider how traditionally prescribed limits on collection, if still applicable,[176] 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.

We may not soon know the full extent to which a user will be able to meaningfully understand the full extent of how their data may be used in a world with cloud-enabled domestic robots. This may mean that it will be necessary to require companies, especially during the

[172] GOVERNMENT 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 (Executive Summary).

[173] *Id.*

[174] See *supra* Part II.B.7; *supra* Part II.C.2.

[175] *See e.g.*, Justin Brookman & G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm*, FUTURE OF PRIVACY FORUM, *available at* http://www.futureofprivacy.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf (articulating five "threat models" for data collection: "data breach, internal misuse, unwanted secondary use, government access, and chilling effect on consumer behavior.").

[176] Policy discussions related to current technological phenomena have caused many to reconsider whether a privacy framework should focus as it has on collection limitations. *See* FRED H. CATE, PETER CULLEN & VIKTOR MAYER-SCHONBERGER, DATA PROTECTION PRINCIPLES FOR THE 21ST CENTURY 15-16 (2013) (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.").

advent of the technology in the consumer space, to presume that consumers are not likely to understand the data practices fundamental to cloud robotics. Unlike other technologies that have had time to develop use norms and customs, the "open world" design of cloud robotics 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, and will instead 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 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[177]—and provide "meaningful" control mechanisms that allow the user to exercise choices regarding the data they disclose to companies. 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 data. Even if data disclosed by a user is within the context of the transaction, the high sensitivity of that data collected and used in a domestic setting could require that companies disclose their data practices and provide easy access for users to exercise choices.[178] However, the time in 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.

[177] *See e.g.*, 2012 FTC PRIVACY REPORT, *supra* note 53, 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)).

[178] *See supra* Part II.C.3 (examining when affirmative expressed consent is required).

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 contemporary FIPPs 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.[179] For many frameworks, the time in which "meaningful" decisions can be made by a user is at the time of, or just prior to, collection. [180] The collection-centric timeframe has typically been utilized to present choices to a consumer because collection, use, and disclosure practices can be halted until a user performs some action, such as consenting to displayed data practices.

Cloud-enabled robots, in which the robot will likely have the autonomy to seamlessly collect, disclose, and use data, may pose challenges to the time in which choices can be 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. 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. 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.[181] Similar to cloud-

[179] *See e.g.*, *supra* Part II.B.2; *supra* Part II.C.3.
[180] *See, e.g.*, WHITE HOUSE PRIVACY REPORT, *supra* note 13, at 11 ("*[A]t the time of collection*, companies should present choices . . ." (emphasis added)).
[181] *See* NEST.COM, https://nest.com/ (last visited March 10, 2014).

enabled robots, Nests systems are located in the home and perform certain actions without constant user interaction.

Unlike devices like Nest, however, which know and communicate to the user what data will be collected and used ahead of time, 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. Nest, for instance, details explicitly what data the "Nest Learning Thermostat" will collect.[182] Cloud-enabled domestic robots' data collection and use practices, on the other hand, will likely not be so finite. Even before taking into consideration the infinite, unforeseen obstacles that may be encountered, the seemingly simple task of fetching a bottle of water would already require "locating a bottle that contains the drink, navigating to the bottle's position on a cupboard, grasping and picking up the bottle, locating the [user] . . . navigating to the [user], and giving the bottle to the [user]."[183] Operating in an unstructured environment may mean that the robot must collect, analyze, and use data, and adapt to situations that may be unforeseen at the time the task is requested. This makes "meaningful" decision-making by a user at the time of collection much more challenging.

An alternative approach, however, is worth highlighting. The FTC Privacy Framework states that, "[i]n some contexts . . . it may be more practical to communicate choices at a later point."[184] 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."[185] This could be the case with cloud robotics, where robots are expected to perform tasks around the home throughout the day while users are busy. In such

[182] *Nest Privacy Statement*, NEST.COM, https://nest.com/legal/privacy-statement/ (last visited March 10, 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 each of these categories entails).

[183] *See, e.g.*, Waibel et. al., *supra* note 8, at 70.

[184] *See* FTC 2012 PRIVACY REPORT, *supra* note 53, at 50.

[185] *Id.*

cases, “the company should wait for a disclosed period of time before engaging in the practices for which choice is being offered.”[186] 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 the choice, it could be considered “relevant” and “meaningful” for future uses of that data, but because tasks cannot be undone, would likely not be considered so for the already completed tasks. 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 time.”[187] In effect, the autonomous functionality of cloud robotics will have us rethink when the appropriate time to disclose relevant data practices and provide meaningful choices will occur.

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 notice and choice mechanisms. Many of the principles underlying contemporary FIPPs 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.”[188] For consumer-facing entities, the physical devices with which consumers interact have consistently been relied upon as the most appropriate place to provide notices and communicate consumer choices. The Consumer Privacy Bill of Rights, specifically, stresses that the disclosure of company data practices should be “easy

[186] *Id.*

[187] FEDERAL TRADE COMMISSION STAFF, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 11 (2013).

[188] 2012 FTC PRIVACY REPORT, *supra* note 53, at 50.

to read *on the devices that consumers actually use to access their services*."[189] The FTC, as well, has relied on the device itself when recommending how mobile application service providers could adhere to the FTC Privacy Framework, suggesting that mobile applications accessing sensitive information "provide 'just-in-time' disclosure of that fact and obtain affirmative express consent from consumers" on the device.[190] This isn't to say that the device is the only sufficient place to communicate data practices to a user,[191] but given its proximity and focal point of interaction with the user, the device has been revered as an appropriate medium through which to communicate relevant disclosures.

Determining how to deliver meaningful choice mechanisms, especially when relying on the physical robot itself, may be challenging for cloud robotics. Cloud enabled-robots are not required to provide an on-board user interface in order to function. For instance, AMIGO, a domestic service robot created at the Eindhoven University of Technology,[192] was used to demonstrate RoboEarth, and did so without an on-board user interface.[193] Computers, tablets, and mobile devices typically provide screens on which to display collection and use practices, allowing "just-in-time" notifications on the screen prior to collection.[194] 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

[189] WHITE HOUSE PRIVACY REPORT, *supra* note 13, at 15 (emphasis added).
[190] FEDERAL TRADE COMMISSION STAFF, *supra* note 187 at 15.
[191] 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). The Future of Privacy Forum's Code of Conduct for retailers utilizing Mobile Location Analytics propose that notice, when required, should be provide to store patrons through "signage that informs consumers about the collection and use of MLA Data at that location." *Id.* at 1–2, *available at* http://www.futureofprivacy.org/wp-content/uploads/10.22.13-FINAL-MLA-Code.pdf .
[192] See *Robots/AMIGO*, ROS.ORG, e (last visited March 10, 2014).
[193] *AMIGO robot downloads its instructions from the RoboEarth internet !*, YouTube, http://www.youtube.com/watch?v=RUJrZJyqftU.
[194] FEDERAL TRADE COMMISSION STAFF, *supra* note 187 at 15.

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."[195] Internet-connected cars, for instance, provide a helpful example. During a recent FTC workshop on the Internet of Things, numerous commenters raised concerns over how to adequately disclose data practices and provide choice mechanisms for products that lack a user interface.[196] AAA, for instance, 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," and could "communicate with consumers via email, phone, or text message (provided the user agrees to such communications)."[197]

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 and entail performing relatively unpredictable movements. While there is no universally accepted definition of "robot," a defining characteristic that is considered in a number of proposed definitions is the ability of the machine to have autonomous mobility.[198] 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 cloud-enabled robot

[195] DANIEL CASTRO & JORDAN MISRA, THE INTERNET OF THINGS 1 (2013), *available at* http://www2.datainnovation.org/2013-internet-of-things.pdf.

[196] Letter from Daniel W. Caprio Jr., counsel for the Transatlantic Computing Continuum Policy Alliance, to Mr. Donald S. Clark, Federal Trade Commission, *Internet of Things, Project No. P135405*, at 2, (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 [are] being collected and may offer controls . . . other technologies will collect and transfer data with little to no recognizable interface . . . ").

[197] *See* Letter from Gerard J. Waldron & Stephen P. Satterfield, Counsel for AAA, to Mr. Donald S. Clark, Federal Trade Commission, *Internet of Things, Project No. 135405*, at 9, (Jan. 10, 2014), *available at* http://www.ftc.gov/sites/default/files/documents/public_comments/2014/01/00012-88249.pdf.

[198] *See, supra* note 18.

happens upon sensitive data that would require consumer choices or consent, it's likely that the user may be nowhere near the robot, and 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 in which to communicate data practices and provide meaningful choices in a context not dependent on the physical robot itself. RoboEarth's architecture does support a Web interface platform "that allows humans to enhance information with the [RoboEarth] database using hypertext mark-up language (HTML) forms."[199] Similar to AAA's suggestion in the connected car context, 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 a cloud-enabled robot's collecting of sensitive data. Overall, cloud-enabled robots may prove to be fertile ground for new understandings of how to properly provide relevant disclosures and meaning choices to consumers.

D. Transparency & Privacy Notices

Providing a conspicuous disclosure of company practices, generally, may be equally difficult for companies producing cloud-enabled domestic robots. Regardless of the sensitivity of data collected by an entity, or the context of a particular transaction, privacy and security practices should be provided by companies in a conspicuous location for privacy-conscience users. Contemporary FIPPs frameworks have recognized some of the shortcomings of traditional privacy notices,[200] 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

[199] Waibel et. al., *supra* note 8, at 75.

[200] *See* Mark MacCarthy, *New Directions in Privacy Disclosures, Unfairness and Externalities*, 6 I/S J. L. & POL'Y FOR 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 too broadly written").

standardized."[201] Determining how to properly articulate the seemingly complex data practices for a cloud-enabled robot in a manner that is easy to understand, clear, and short 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 choices mechanisms. Clear disclosures will unlikely be able to communicate with any specificity the data that will be collected, and the manner in which it may be used, due to the autonomous nature of cloud-enabled robots operating in unstructured environments. Additionally, efforts to make these notices clearer, shorter, and more standardized could leave out important practices that should have been communicated to users, reflecting what some call the "transparency paradox."[202]

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. Modern technologies are currently struggling with this problem. The GAO Report, described above, also found that auto manufacturers, portable navigation device companies, and developers of map and navigation applications for mobile devices "have taken steps" to adopted industry-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."[203] 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

[201] *See supra* Part II.B.3; *supra* Part II.C.4.
[202] Helen Nissenbaum, *A Contextual Approach to Privacy Online*, DÆDALUS, J. AM. ACAD. ARTS & SCI. 32, 34 (2011).
[203] GOVERNMENT ACCOUNTABILITY OFFICE, *supra* note 172.

"broadly worded."[204] Companies providing 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. 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.[205] Early efforts to standardize cloud robot 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.[206] The adoption of "visceral notice," for instance, in which physical sensations and experience communicate information to a user, may be a unique approaches for cloud-enabled robots to provide notice to users of data collection and use practices.[207]

E. Security

While cloud robotics may not necessarily pose unique challenges to securing data, the sensitivity of data collected, used, and retained by cloud-enabled robots will likely place added pressure on companies to secure its data and its networks.[208] Contemporary FIPPs frameworks

[204] *Id.*

[205] *See* 2012 FTC PRIVACY REPORT, *supra* note 53, at 61–63.

[206] Ryan Calo, *Against Notice Skepticism in Privacy (And Elsewhere)*, 87 NOTRE DAME L. REV. 1027, (arguing "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").

[207] *Id.* at 1034–1046 (examining possible ways to deliver visceral notices).

[208] *See* Calo, *supra* note 15, 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").

call for some form of "reasonable" or "responsible" data security practices.[209] That being said, many frameworks intentionally refrain from stating what specific security practice would be "reasonable" or "responsible," and instead highlight that "industry best practices and standards" would provide the basis for reasonable security practices. Some states have established reasonable data security practices through regulation,[210] while the Federal Trade Commission has highlighted "reasonable" practices within its Section 5 complaints against companies accused of "unfair" data security practices.[211] Many entities have also developed their own technology-centric approaches to data security.[212] Cloud robotics will likely be able to adopted existing security standards for data traveling over its networks,[213] however, the sensitivity of data collected, used, and retained by cloud-enabled robots will make the consequences of any compromised cloud robot networks or databases so significant that companies will be required to go beyond current best practices. 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.[214]

F. Access & Accuracy

Companies providing cloud-enabled domestic robots will also need to determine how they can maintain the accuracy of the data they collected, as well as the extent to which users can

[209] *See supra* Part II.B.5; supra Part II.C.2.
[210] *See* M.G.L.A. 93H § 2; Mass. 201 CMR 17 17.03 (detailing requirements for "reasonable data security")
[211] *See, e.g.*, In re of TRENDnet, Inc., Complaint, File No. 122 3090 (2013) (alleging TRENDnet "[f]ail[ed] to employ reasonable and appropriate security in the design and testing of the software utilized in its cameras").
[212] *See e.g.*, CENTER FOR DEMOCRACY & TECHNOLOGY, BEST PRACTICES FOR MOBILE APPLICATIONS 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).
[213] For instance, RoboEarth states that its data "[are] made available via standard Internet protocols" Waibel et. al., *supra* note 8, at 71. Contemporary encryption methods and similar security practice for such protocols could be utilized within the cloud architecture.
[214] Such an approach could follow approaches taken within other areas of robotics. *See, e.g.*, ROBOTIC INDUSTRIES ASSOCIATION, NEW ROBOT SAFETY STANDARDS 1 (2013), *available at* http://www.robotics.org/content-detail.cfm/Industrial-Robotics-News/New-Robot-Safety-Standard/content_id/4133 (establishing "American national robot safety standards" for robot manufactures and integrators).

access the data collected and stored. Contemporary FIPPs 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.[215] The right to access has been a core of the FIPPs since first articulated within the Department of Health, Education and Welfare Report,[216] however, the increasing ubiquity of data has caused many to rethink the extent to which access should be provided to users. Some have found that increased access to data, regardless of the technology, is critical "in an environment where consent is not always possible or feasible."[217] Others, however, are less persuaded by the advantages and benefits that providing access may have for users.[218] As cloud robotics becomes more advanced, it many need to understand not only how information is to be collected and analyzed by a robot, but also the impact that information is to going to have on the user. While inaccurate information in the robot database may not be as harmful as inaccurate credit information, the impact could still be significant. Methods of access to data collected and stored by a cloud-enabled robot could not only satisfy access principles, but could also provide an increased level of individual control over the information within a cloud robot database.[219]

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

[215] *See supra* Part II.B.6; *supra* Part II.C.2–3.

[216] *See supra* note 38 & accompanying text.

[217] David A. Hoffman *Putting Privacy First in Big Data Technologies*, RE/CODE, Feb. 10, 2014, http://recode.net/2014/02/10/putting-privacy-first-in-big-data-technologies/.

[218] *See* THOMAS M. LENARD & PAUL H. RUBIN, THE BIG DATA REVOLUTION: PRIVACY CONSIDERATIONS 20 (2013), *available at* https://www.techpolicyinstitute.org/files/lenard_rubin_thebigdatarevolutionprivacyconsiderations.pdf.

[219] 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, HÄUSSERMANN, & ZWEIGLE, *supra* note 150, at 15.

contemporary FIPPs frameworks. The principle of Accountability requires companies to be accountable for complying with its respective FIPPS framework.[220] Yet, as some have observed, creating and enforcing accountability "is increasingly difficult given the external pressure for increased flexibility in design of rules."[221] With so many FIPPs 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."[222] Proper accountability will only be possible if and when companies providing cloud-enabled domestic robots understand how best to adhere to contemporary FIPPs frameworks. Once effective practices are in place, cloud-enabled techniques, such as audits, evaluations, and privacy impact assessments will need to be utilized in order for companies to determine what specific privacy objectives are required or desired, and whether or not those objectives have been achieved.

IV. APPROACHING THE PRIVACY CHALLENGES INHERIT IN CONSUMER CLOUD ROBOTICS

By examining some of the contemporary approaches to the FIPPs, 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 of course, the overarching 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. By recognizing the possible inconsistencies that may result from applying contemporary FIPPs

[220] *See, e.g.*, *supra* Part II.B.8.
[221] WORLD ECONOMIC FORUM, *supra* note 163, at 17.
[222] *Id.* at 3.

frameworks to cloud robotics concepts companies can have the added advantage of being able to adjust, amend, or emphasize certain practices in order to respect consumer privacy.[223] "An ounce of prevention," as they say, "is worth a pound of cure."[224]

Recognition of these challenges, however, does not necessarily require finding immediate solutions to them. A productive future starts with asking the right questions. Tamara Denning 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.[225] The research uncovered significant security vulnerabilities that could allow an attacker to intercept or inject wireless packets into some of the tested household robots.[226] 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.[227] Some of these proposed questions are basic design questions, such as "how mobile is the robot" and "what is the robot's intended operational environment," while more complex questions included, "does the robot create new or amplified existing privacy vulnerabilities?"

An approach similar to Denning's method of "recognizing the challenge" and "presenting questions and suggestions" to overcome privacy concerns could prove valuable, not only from a design perspective, but from a law and policy perspective. Consider, for example, the FIPPs' focus on "context." As this Paper has explained, understanding the context in which a user may

[223] *See* Denning et. al., *supra* note 12, 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").
[224] *Fire Department: The Electric Ben Franklin*, USHISTORY.ORG, http://ww.ushistory.org/franklin/philadelphia/fire.htm (last visited March 10, 2014) (attributing this quote to Benjamin Franklin).
[225] *See* Denning et. al., *supra* note 12.
[226] *Id.* at 107–109.
[227] *Id.* at 113.

disclose their data at the advent of cloud robotics may be extremely difficult, yet this is a significant component to contemporary FIPPs frameworks.[228] 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.

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.[229] The study identifies variables which 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 users' trust in the service provider, the method of collection, and the device used.[230]

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. 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.[231] The study suggested, 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

[228] *See supra* Part III.B.
[229] INTERNATIONAL INSTITUTE OF COMMUNICATIONS, PERSONAL DATA MANAGEMENT: A 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.
[230] *See id.* at 15–25.
[231] *See id.* at 12–13, 20–21

value exchanged for their data," "they are provided with clear insights into how the data [are] being collected and how [they are] being used," and "they have control over the types of data being collected, accessed and used."[232] Considering the dependence cloud robotics will have on "passively collected data," such recommendations could be a starting point for discussion as companies contemplate how cloud-enabled robots may emerge as a consumer product. This is just one example. 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-enabled robots 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. Individuals within the robotics community should become familiar with the "heated debate" over current U.S. information privacy law.[233] Some regulators and advocates are continuously calling on Congress to propose legislation that would "close the gaps" within consumer privacy.[234] Others, however, are against any regulatory reform, and believe industry self-regulation would be sufficient.[235] It is doubtful that 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

[232] *Id.* at 22.
[233] *See* Bamberger & Milligan, *supra* note 50 at 254–63.
[234] *See, e.g.*, Julie Brill, Commissioner, Federal Trade Commission, 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.")
[235] *See* Adam Theier, *Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle*, 14 MINN. J. L. SCI. & TECH. 309 (2013).

unique perspective on tomorrow's technologies and avoid hindering the cloud robotics infrastructure or ecosystems.[236]

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."[237] Software developers and roboticists who have a solid understanding of what practices can mitigate consumer privacy concerns from a law and policy perspective would 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,[238] 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 cloud robotics. Growth in this area is well underway. A number of law firms have begun to invest in practice areas focusing on robotics.[239] The "We Robot" Conference, now in its third

[236] Such a "call to arms" has started in the Big Data context. During Federal Trade Commission 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 computer scientists "to help create technological solutions to some of the most vexing privacy problems presented by big data." Julie Brill, Commissioner, Federal Trade Commission, Sloan Cyber Security Lecture at the Polytechnic Institute of NYU (Oct. 23, 2013).

[237] 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 Federal Trade Commission's Privacy Framework explicitly advocates a "Privacy By Design" approach. *See supra* Part II.C.2.

[238] *See* Podsiadła, *supra* note 16.

[239] *See e.g., Robotics, AI and Automation*, LITTER MENDELSON P.C., http://www.littler.com/practice-areas/robotics-ai-and-automation (last visited March 13, 2014) (focusing its practices on robotics within a workplace environment); Practice *Areas: Robotics and Artificial Intelligence*, COOKE KOBRICK & WU, http://www.ckwlaw.com/practice-areas/Robotics_and_Artificial_Intelligence/ (last visited March 13, 2014); *see also* Ryan Calo, *Even (Some) Law*

year, has started to encourage discussion and collaboration on the law and policy issues surrounding robotics.[240] The American Bar Association Section of Science & Technology Law has also formed a committee on Artificial Intelligence and Robotics.[241] In addition, legal scholars have begun to contribute meaningful scholarship to the robotics field, not as satirical hypotheticals, but as meaningful contributions to how robotics will begin to adapt to our country's legal landscape.[242]

Going forward, collaboration will help recognize the privacy concerns of could robotics while providing a better understanding of how contemporary FIPPs frameworks can meaningfully address potential consumer privacy concerns associated with cloud-enabled robots. As Peter Swire and Annie Anton have stated,

> Organizations 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.[243]

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

Firms Think Robots Are The Next Big Thing, FORBES.COM, Jan. 31, 2014, *available at* http://www.forbes.com/sites/ryancalo/2014/01/31/even-some-law-firms-think-robots-are-the-next-big-thing/.

[240] *See About We Robot*, WE ROBOT, http://robots.law.miami.edu/ (last visited March 13, 2014).

[241] *See Section of Science & Technology Law: Artificial Intelligence and Robotics Committee*, AMERICAN BAR ASSOCIATION, http://apps.americanbar.org/dch/committee.cfm?com=ST248008, (last visited March 13, 2014).

[242] *See, e.g.*, Calo, *supra* note 170 (examining the commercial implication of "open" or "closed" robotics); Dan Terzian, *The Right to Bear (Robotic) Arms*, 117 PENN ST. L. REV. 755 (2013) (examining the Second Amendment implications of robotic weapons and robots wielding firearms).

[243] Peter Swire & Annie Antón, *Engineers and Lawyers in Privacy Protection: Can We All Just Get Along?*, PRIVACY PERSPECTIVE, Jan. 31, 2014, *available at* https://www.privacyassociation.org/privacy_perspectives/post/engineers_and_lawyers_in_privacy_protection_can_we_all_just_get_along.

preventing disclosure, and can begin to improve internal systems and focus on privacy-enhancing technologies that respect and adhere to contemporary FIPPS practices. 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 would allow robots to be smaller, cheaper, and more efficient in interacting within unstructured, open environments. As cloud robotics continues to advance, 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 comes with a number of legal, technical, societal, and of course, privacy challenges. Consumer protection in the United States today has involved a comingling of sector-specific regulations and proposed industry best practices founded on the Fair Information Practice Principles. Though contemporary privacy frameworks, including the White House's Consumer Privacy Bill of Rights and the Federal Trade Commission's Privacy Framework, have attempted to properly balance consumer expectations with appropriate respect to advancements in technology, challenges will likely occur when these frameworks are applied to an emerging technology like cloud robotics.

As more data become necessary for cloud-enabled robots to operate in unstructured environments, questions begin to arise, such as 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, what exactly will determine the limits on data collection, use, and retention practices? More importantly, when and how can companies communicate "meaningful" and "relevant" 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 requires collection or use? Posing these questions may help 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.