2017 IEEE 37th International Conference on Distributed Computing Systems Workshops

Towards Privacy-Aware Smart Buildings: Capturing, Communicating, and Enforcing Privacy Policies and Preferences

Primal Pappachan*, Martin Degeling†, Roberto Yus*, Anupam Das†,
Sruti Bhagavatula†, William Melicher†, Pardis Emami Naeini†, Shikun Zhang†,
Lujo Bauer†, Alfred Kobsa*, Sharad Mehrotra*, Norman Sadeh†, and Nalini Venkatasubramanian*
* *University of California Irvine*
Email: {primal, ryuspeir, kobsa}@uci.edu, {sharad, nalini}@ics.uci.edu
† *Carnegie Mellon University*
Email: {degeling, anupamd, shikunz, sadeh}@cs.cmu.edu, {srutib, billy, pardis, lbauer}@cmu.edu

***Abstract*—The Internet of Things (IoT) is changing the way we interact with our environment in domains as diverse as health, transportation, office buildings and our homes. In *smart building* environments, information captured about the building and its inhabitants will aid in development of services that improve productivity, comfort, social interactions, safety, energy savings and more. However, by collecting and sharing information about building's inhabitants and their activities, these services also open the door to privacy risks.**

In this paper, we introduce a framework where *IoT Assistants* capture and manage the privacy preferences of their users and communicate them to *privacy-aware smart buildings*, which enforce them when collecting user data or sharing it with building services. We outline elements necessary to support such interactions and also discuss important privacy policy attributes that need to be captured. This includes looking at attributes necessary to describe – (1) the data collection and sharing practices associated with deployed sensors and services in smart buildings as well as (2) the privacy preferences to help users manage their privacy in such environments.

I. Introduction

The Internet of Things (IoT) is upon us. From smart cars to smart buildings and from activity bracelets to smart fridges, every object in our environment is increasingly being endowed with sensing, computing, communication, and actuation functionalities. This rapid transformation of the world we live in is opening the door to many potential benefits. One domain where this transformation is taking hold is *smart buildings*. Here traditional HVAC (heating, ventilating, and air conditioning) systems are being enhanced with functionalities that ties to beacons, presence sensors, cameras and personal devices such as smartphones carried by the building's inhabitants. One commonality to all these new technologies and scenarios is their reliance on the collection of data that contradicts the expectations of privacy. Therefore, while the advent of IoT holds many promises, it also gives rise to new and complex privacy challenges. Various studies have demonstrated that by observing electrical events and cell phone usage in a space it is possible to detect the whereabouts and daily activities of its residents [1], [2], [3]. This problem has been recognized at the highest level, including in the form of guidelines developed by the OECD[1] and reports from the Federal Trade Commission[2]. These challenges have also lead to studies and design of frameworks to model and enforce people's privacy preferences [4], [5].

Compared to other mediums such as the traditional Web, where users consciously navigate from one website to the next, in IoT environments such as smart buildings users are less likely to be aware of the technologies with which they might be interacting. Our approach is intended to remedy this situation by providing an interface where users can discover technologies in their surroundings and the privacy ramification of interacting with these technologies. As has been reported by McDonald and Cranor, even on the fixed Web, users do not read privacy policies [6]. In an IoT context, it is even more imperative to have mechanisms that can notify user about relevant privacy policies and help them manage their privacy preferences. Along with these, IoT system should be capable of efficiently enforcing privacy policies and preferences from different users without loss of utility for the services that exist in the space.

In this paper, we describe a framework for smart buildings which includes three main components. First, *IoT Resource Registries* (IRRs) which broadcast data collection policies and sharing practices of the IoT technologies with which users interact. Second, *IoT Assistants* which selectively notify users about the policies advertised by IRRs and configure any available privacy settings. Third, *privacy-aware smart buildings*, which publish building policies (e.g., through IRRs), receive the privacy settings of users (e.g., from IoTAs) and enforce them when collecting user data or sharing it with services. A first version of this framework has been implemented and deployed in the Donald Bren

[1]https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf
[2]https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices

2332-5666/17 $31.00 © 2017 IEEE
DOI 10.1109/ICDCSW.2017.52

Hall at University of California Irvine and is concurrently undergoing deployment at Carnegie Mellon University.

The rest of the paper is organized as follows. In Section II, we describe the need for privacy-aware smart buildings and outline how users can rely on their IoTAs and on the presence of one or more IRRs to manage their privacy in a smart building. In Section III, we present building privacy policies and user privacy preferences and present examples in the context of smart buildings. Section IV presents the elements required to represent such policies and user preferences followed by an overview of the language. Challenges associated with the development and deployment of our infrastructure, including ongoing work are further discussed in Section V.

II. Overview of Smart Buildings

Building Management Systems (BMS) are cyber-physical systems that are used to manage buildings by monitoring different utility services. As an example, Donald Bren Hall (DBH) is a 90 000+ square feet 6-story building at University of California, Irvine (UCI) equipped with a BMS. DBH is equipped with more than 40 surveillance cameras covering all the corridors and doors (for security purposes), 60 WiFi Access Points (AP) (for Internet connectivity), 200 Bluetooth beacons (for broadcasting information of interest to inhabitants), and 100 Power outlet meters (for monitoring energy usage).

A. Privacy Threats in Current Smart Building Scenarios

BMS capture a digital representation of a dynamically evolving building at any point in time for purposes such as comfort and security. But this representation might contain distinct patterns which can reveal the absence or presence of people and their activities, potentially resulting in the disclosure of data that people might not feel comfortable disclosing (e.g., where they go, what they do, when and with whom they spend time, whether they are healthy and more) [7]. For example, when a user connects to a WiFi AP in DBH, this event is logged for security purposes (the information logged includes the MAC address of the device and AP, and a timestamp) as part of the *building policy*. Using background knowledge (e.g., the location of the AP) it is possible to infer the real-time location of a user. Also, using simple heuristics (e.g., non-faculty staff arrive at 7 am and leave before 5 pm, graduate students generally leave the building late, and undergrads spend most of the time in classrooms), it is possible to infer whether a given user is a member of the staff or a student. Furthermore, by integrating this with publicly available information (e.g., schedules of professors and the courses they teach or event calendars), it would be possible to identify individuals. Some people may not object to such data collection, while others might. One challenge associated with privacy is that often not all users feel comfortable about the same data practices. Therefore, it is important to understand *user preferences* and *expectations* with respect to the information collected and used by a system like BMS [8], [9].

B. Privacy-Aware Smart Buildings

Adapting current building management systems to handle policies and user preferences is a complex task. Currently, we are developing a privacy-aware smart building testbed (*TIPPERS* [10] [11]) which captures raw data from the different sensors in the building, processes higher-level semantic information from such data, and empowers development of different building services. TIPPERS is also capable of capturing and enforcing privacy preferences expressed by the building's inhabitants. These preferences are captured by, for example, each user's *IoT Assistant* [12], which in turn uses them to configure available privacy settings - whether automatically or via interactions with the user. This interaction is explained below.

C. User Interactions in Privacy-Aware Smart Buildings

Figure 1 outlines how a user (who will be referred to as *Mary* from now onward for ease of explanation) interacts with this infrastructure. The building admin of DBH uses the smart building management system (such as TIPPERS) to define policies regarding the collection and management of data within the building (step (1) in Figure 1). Based on these policies, the different sensors in the building are actuated and data from them, some of which might be related to its inhabitants (step (2)), is captured and stored (step (3)). These policies are made publicly available through one or more IoT Resource Registries (step (4)). As Mary walks into the building carrying her smartphone with IoTA installed on it, the IoTA discovers available registries that pertain to resources in her vicinity and obtains machine-readable privacy policies detailing the practices of resources close to her location (step (5)). The IoTA displays summaries of relevant elements of these policies to the user (step (6)) by focusing on the elements of a policy that are important respect to the users privacy preferences. This is done using a model of Mary's privacy preferences learned over time. This might include information about those data collection and use of practices she cares to be informed about (step (7)). If a policy identifies the presence of settings, the IoTA can also use knowledge of Mary's privacy preferences to help configure these settings by communicating with TIPPERS (e.g., submitting requests to change settings) (step (8)). If a service later requests TIPPERS about Mary's location (step (9)), the request will be processed according to the settings communicated by Mary's IoTA to TIPPERS (e.g., the request might be rejected, if Mary's IoTA requested to opt-out of location sharing; step (10)).

To implement this interaction, we designed a machine-readable policy language as a mechanism to capture and

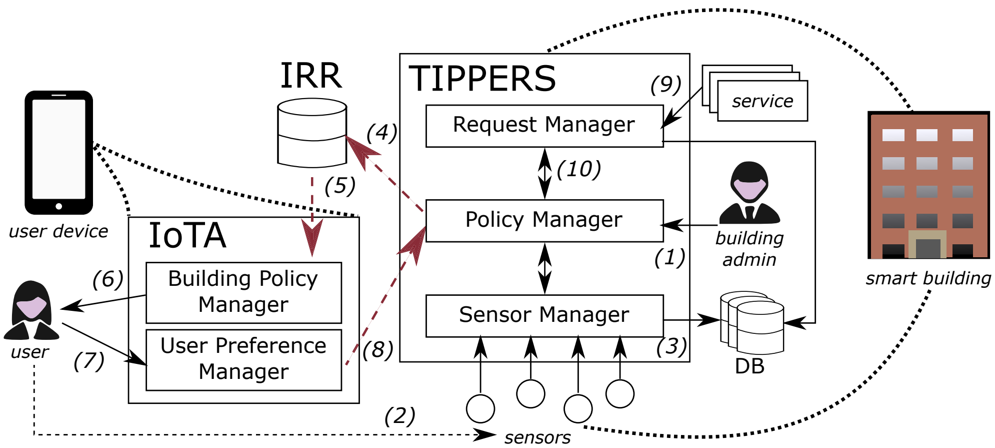

Figure 1: Interaction between privacy-aware smart building management system (TIPPERS), IoT Resource Registries (IRR) and IoT Assistants (IoTA).

communicate building policies of smart buildings to its inhabitants. The policy language is used to convey users' preferences and settings to the smart building sytem through an IoTA. In the interaction described above different elements could use the language to advertise building policies (step (4)), match them with the user preferences (step (5)), and communicate the matched user preferences to the building system (step (8)).

III. Facets of a Privacy-Aware Smart Building Infrastructure

Building policies and user preferences are important to ensure that a smart building systems meets the privacy needs of its inhabitants. In this section, we explain both building policies and user preferences in detail with examples.

A. Building Policies

A *building policy* states requirements for data collection and management set by the temporary or permanent owner. Building policies can be related to the infrastructure of the building, specific sensors deployed in the building or even events taking place inside the building. These policies (in most cases) have to be met completely by the other actors in the pervasive space. Here are some examples of building policies that can be entered into TIPPERS and advertised by the IRR.

- *Policy 1*: A facility manager sets the thermostat temperature of occupied rooms to 70°F to match the average comfort level of users.
- *Policy 2*: The building management system stores your location to locate you in case of emergency situations.
- *Policy 3*: A building administrator defines that either an ID card or fingerprint verification is needed to access meeting rooms.
- *Policy 4*: An event coordinator requires that details regarding an event are disclosed to registered participants only when they are nearby.

To implement these policies, they have to be translated into settings that change the state of sensors. For example to execute *Policy 1* it is necessary to *i*) make a request to motion sensors in each room to determine whether the room is occupied or not, *ii*) pull information from temperature sensors to determine whether the HVAC system has to be activated, and *iii*) change the settings of the HVAC system to increase or decrease the fan speed to adjust the temperature.

B. User Preferences

Building policies support building management but at the same time put user's privacy at risk. For example, using the data collected based on *Policy 1* it is possible to discover whether someone's office is occupied or not which in turn can be used to learn the occupant's working pattern. Therefore, in smart buildings, users should be able to express their privacy preferences regarding the data collected by the building.

A *user preference* is a representation of the user's expectation of how data pertaining to her should be managed by the pervasive space. These preferences might be partially or completely met depending on other policies and user preferences existing in the same space. Some examples of user preferences are:

- *Preference 1*: Do not share the occupancy status of my office in after-hours.
- *Preference 2*: Do not share my location with anyone.

Smart buildings such as DBH also provide services, built on top of the collected sensor data, to the inhabitants of the building. Two examples of such services operating at DBH are 1) *Smart Concierge* service, which helps users locate rooms, inhabitants and events in the building, 2) *Smart*

Meeting service, which can help organize meetings more efficiently. These services take information from the user captured by the building (e.g., their current location) and return interesting information (e.g., nearest coffee machine). In addition to services provided by the building, there could be other third-party services running on top of the smart building management system. For example, a food delivery company can automatically locate and deliver food to building inhabitants during lunch time.

While using a service inside the building, a user can also specify her policies in the form of permissions allowed for the service. This is similar to how the permissions are managed in mobile apps. This allows a user to directly review what information the service requests and for what purpose. For the previously described services (in Section III-A), possible user permissions could be

- *Preference 3*: Allow *Concierge* access to my fine grained location for directions
- *Preference 4*: Allow *Smart Meeting* access to the details of the meeting and its participants.

It is possible that user preferences conflict with the existing building policies (e.g., *Policy 2* and *Preference 2*). These conflicts should be detected by the smart building management system (e.g., with the help of a policy reasoner) which is in charge of enforcing the policies by resolving these conflicts while informing users about it through the personal privacy assistant.

IV. Communicating Policies and Preferences

Building policies and user preferences have context specific requirements that need to be captured and communicated in a flexible manner. In this section, we first describe the various elements of our machine-readable policy. Second, we describe a high-level language schema that can be used to capture such policy.

A. Building Specific Policy Elements

There are different elements in a building that have to be represented in policies such as space, users, sensors and services. For the elements described below, we use existing ontologies if available.

1) Spatial Model: includes information about infrastructure, such as buildings, floors, rooms, corridors, and is inherently hierarchical. The spatial model also supports operators such as "contained", "neighboring", and "overlap".

2) User Profile: models the concept of people in the environment. Profiles can be based on groups (students, faculty, staff etc.) and share common properties (e.g., access permissions). A user can have multiple profiles which includes information such as department, affiliation, and office assignment in our sample scenario.

3) Sensor: describes the entity which captures information about its environment. Each sensor has a sensor type and can produce a reading based on its type. Sensors of the same type can be organized into sensor subsystems. Examples of such subsystems are camera subsystem, beacon subsystem, and HVAC subsystem (modelled using the haystack[3] ontology and Semantic Sensor Network ontology [13]).

4) Settings of a sensor: is a set of valid parameters associated with the sensor which determines its behavior (e.g., for a camera it could be the capture frequency or the resolution of the image). A sensor is actuated based on the parameters specified in its current settings. A sensor can have multiple settings dictated by its type.

5) Observation: models the type of data captured by a sensor based on the type and settings associated with it. Each observation has a timestamp and a location (determined based on whether the sensor is mobile or fixed) associated with it.

6) Service Model: describes the services that run on top of smart building systems and provide interesting information to the users. The service model captures meta-data about the service such as the developer (e.g., building owner or third party), permissions to sensors, and observations. This model also describes details about the service itself such as the information returned or functionality provided.

B. Privacy Specific Policy Elements

While building and sensor specific models can capture information about different entities, there is a need for a description of the data collection practices in a building from the perspective of a user. Peppet [14] analyzed privacy policies of companies that manufacture IoT devices and concluded that through these policies, users not only want to be informed about what data is collected by which devices and for what purposes, but also about the granularity of data collection (whether or not it is aggregated or anonymized) and with whom the data is shared. Based on this, we introduce the following policy elements to model a user's privacy settings.

1) Context: describes meta information about the building and the BMS that point users to general information (e.g., who is responsible for data collection in a building, where are sensors located, and whom to contact when it comes to questions regarding the policy). This meta information can also contain a general description of data security and ownership of information which are relevant to the user.

2) Data collected and inferred: While the observation model captures information about the data collected, a user might be more interested in knowing what can be inferred from the collected data. Therefore, it is important to specify the abstract information that can be inferred from an observation captured by a sensor. For example, to model the

[3]http://project-haystack.org

occupancy of a room, it would be better to describe it as "if a room is occupied by anyone" compared to an observation model which might only have information such as "images from camera", "logs from WiFi APs", etc. Data collection description also contains information about the granularity of the data collected as granularity can directly impact the capability of inference.

3) Purpose: models the requirement of data collection which is closely related to a service that uses this data. In a BMS, some data collections such as temperature monitoring serves a straightforward purpose for setting the thermostat, but for other data collections such as the information of connecting to WiFi APs can be used for different purposes (e.g., for logging as well as to track the location of a particular MAC address). We are currently working on a taxonomy to model purpose which includes information about whether or not the data is shared (e.g., with law enforcement officers for security purposes) and for how long it will be stored (i.e., retention).

C. Overview of the Language Schema

Based on the aforementioned elements, we are designing a language schema that is capable of capturing both building policies and user preferences. In the following we give an overview of the language by representing some of the examples from Section III. We use a JSON-Schema v4[4] for the representation. We choose JSON over other formats mainly because of the rapid adoption of JSON-based REST APIs.

Figure 2 shows how *Policy 2* ("Location tracking for emergency response") can be expressed using the language. The first part of the language expresses the general information about the location and sensor type (in this case location is DBH at UCI with WiFi APs being the sensors) whereas the second part expresses the data collection purpose (emergency response), data type, and retention period of the data itself.

In case of the policies related to services such as the *Smart Concierge* (as mentioned in Section III-A) can be expressed as shown in Figure 3. The first part describes the information required by the service and the second part shows the purpose of collecting this information.

Concerning user's preference settings, the language can express choices related to policies and services. In the context of *Smart Concierge* service, Figure 4 shows options for the different granularities at which location data can be collected. Thus, if a user is comfortable with sharing fine-grained location data with the Concierge service for directions then our language can capture such *Preference*.

V. Discussion

We presented a template for future smart buildings which includes privacy-aware building management systems and

[4]http://json-schema.org

```
{"resources": [{
  "info": { "name": "Location tracking in DBH" },
  "context": {
    "location": {
      "spatial": {
        "name": "Donald Bren Hall",
        "type": "Building"
        },
        "location_owner": {
          "name": "UCI",
          "human_description": {
            "more_info": "http://ics.uci.edu"
          }}},
    "sensor": {
      "type": "WiFi Access Point",
      "description": "Installed inside the building and
           covers rooms and corridors"
  }},
  "purpose": {
    "emergency response": {
      "description": "Location is stored continuously"
  }}
  "observations": [{
    "name": "MAC address of the device",
    "description": "If your device is connected to a WiFi
         Access Point in DBH, its MAC address is stored"
   }],
  "retention": {
    "duration": "P6M"}}]}
```

Figure 2: Policy related to data collection inside DBH.

```
{"observations": [{
  "name": "wifi_access_point",
  "description": "Whenever one of your devices connects to
       the DBH WiFi its MAC address is stored"
  }, {
  "name": "bluetooth_beacon",
  "description": "When you have Concierge installed and
       your bluetooth senses a beacon, the room you are in
       is stored"}],
"purpose": {
  "providing_service": {
    "description": "Your location data is used to give you
         directions around the Bren Hall."},
  "service_id": "Concierge"}}
```

Figure 3: Policy related to a service in the building.

```
{"settings": [
  {"select": [
    {"description": "fine grained location sensing",
     "on": "http://tippers/user/concierge?beacon=opt-in&
          wifi=opt-in"},
    {"description": "coarse grained location sensing",
     "on": "http://tippers/user/concierge?beacon=opt-out&
          wifi=opt-in"},
    {"description": "No location sensing",
     "on": "http://tippers/user/concierge?beacon=opt-out&
          wifi=opt-out"}]}
```

Figure 4: Privacy settings available.

IOT assistants and can give users better control over the information that buildings collect about them. We described the requirements and elements of a machine-readable language required for this collaboration, which can represent building policies and user preferences. However, to make this vision of a building that takes user privacy into account a reality, many challenges have to be tackled. In the following, we discuss some of the challenges that we are focusing in our on-going work.

A. Policy Specifications

The development of abstract models to allow the specification of policies for different contexts is in progress. We are exploring the trade-off between specificity in language which allows for automated enforceable building policies and preferences versus allowing ambiguity so that they are similar to natural language privacy policies [15]. In our future work we want to address the representation of data handling practices, like the purpose of data collection, in ways that are both expressive enough and enable automatic reasoning to detect conflicts with user preferences.

B. Designing IoT Assistants

While an IoT Assistant can help users in understanding the policies broadcast by the smart building, identifying which privacy practices are most relevant to users is important [16], [9]. This requires a unified way to discover IoT technologies through IRRs and we envision that the setup of IRRs can be automated (e.g. by leveraging Manufacturer Usage Descriptions [17]).

Second, an IoTA could make recommendations to users following an approach similar to the work done by Liu et al. [8] for mobile applications. For such a mechanism to work correctly, the assistant requires labeled data over a period of time to decipher the patterns in a user's behavior and represent them as preferences for the user. Therefore, the challenges include when and how to notify a user and how to obtain user feedback without inducing user fatigue.

C. Developing Privacy-Aware Smart Buildings

The high-level policies and preferences have to mapped into appropriate entities in the building space before their enforcement. This mapping determines the *where* (at devices or BMS), *when* (during capture, storage, processing, or sharing) and *how* (accept/deny data access or add noise) these policies and preferences should be enforced on the user data. The possibilities for customization in this mapping, and thus expressibility of policies and preferences, are decided by the capabilities of privacy-aware buildings.

With large number of users, services, policies, and preferences the cost of enforcement can be large enough to be prohibitive in any real setting. To overcome this challenge, we are working on techniques for optimizing enforcement so that the overhead of privacy compliance is minimized in such systems.

Acknowledgement

This material is based upon work supported by NSF under grant NSF-1450-768 and by DARPA under grants FA8750-16-20021 and FA8750-15-2-0277.

References

[1] M. Berenguer, M. Giordani, F. Giraud-By, and N. Noury, "Automatic detection of activities of daily living from detecting and classifying electrical events on the residential power line," in *10th Int. Conf. on e-health Networking, Applications and Services (HealthCom)*, 2008, pp. 29–32.

[2] M. A. Lisovich, D. K. Mulligan, and S. B. Wicker, "Inferring personal information from demand-response systems," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 11–20, 2010.

[3] N. Eagle and A. S. Pentland, "Reality mining: sensing complex social systems," *Personal and ubiquitous computing*, vol. 10, no. 4, pp. 255–268, 2006.

[4] M. Langheinrich, "Privacy by design - principles of privacy-aware ubiquitous systems," in *Int. Conf. on Ubiquitous Computing*, 2001, pp. 273–291.

[5] N. M. Sadeh, F. L. Gandon, and O. B. Kwon, "Ambient Intelligence: The MyCampus Experience," Tech. Rep., 2005.

[6] A. McDonald and L. Cranor, "The cost of reading privacy policies," *IS: A Journal of Law and Policy for the Information Society*, pp. 540–565, 2009.

[7] M. Benisch, P. G. Kelley, N. Sadeh, and L. F. Cranor, "Capturing location-privacy preferences: quantifying accuracy and user-burden tradeoffs," *Personal and Ubiquitous Computing*, pp. 679–694, 2011.

[8] B. Liu, M. S. Andersen, F. Schaub, H. Almuhimedi, S. A. Zhang, N. Sadeh, Y. Agarwal, and A. Acquisti, "Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions," in *12th Symposium on Usable Privacy and Security (SOUPS)*, 2016, pp. 27–41.

[9] A. Rao, F. Schaub, N. Sadeh, A. Acquisti, and R. Kang, "Expecting the Unexpected: Understanding Mismatched Privacy Expectations Online," in *12th Symposium on Usable Privacy and Security (SOUPS)*, 2016, pp. 77–96.

[10] S. Mehrotra, A. Kobsa, N. Venkatasubramanian, and S. R. Rajagopalan, "TIPPERS: A privacy cognizant IoT environment," in *2016 IEEE Int. Conf. on Pervasive Computing and Communication Workshops (PerCom Workshops)*, 2016.

[11] http://tippersweb.ics.uci.edu.

[12] http://privacyassistant.org.

[13] M. Compton, P. Barnaghi, L. Bermudez, R. GarcíA-Castro, O. Corcho, S. Cox, J. Graybeal, M. Hauswirth, C. Henson, A. Herzog *et al.*, "The ssn ontology of the w3c semantic sensor network incubator group," *Web semantics: science, services and agents on the World Wide Web*, vol. 17, pp. 25–32, 2012.

[14] S. R. Peppet, "Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security and Consent," *Texas Law Review*, vol. 93, p. 85, 2014.

[15] J. R. Reidenberg and L. F. Cranor, "Can user agents accurately represent privacy policies?" *Social Science Research Network*, 2002.

[16] J. Gluck, F. Schaub, A. Friedman, H. Habib, N. Sadeh, L. F. Cranor, and Y. Agarwal, "How Short Is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices," in *12th Symposium on Usable Privacy and Security (SOUPS)*, 2016, pp. 321–340.

[17] E. Lear, R. Droms, and D. Romascanu, "Manufacturer Usage Description Specification," IETF Network Working Group, Internet-Draft, Feb. 2017.