An overview of user privacy preferences modeling and adoption

Georgia M. Kapitsaki*, Alexia Dini Kounoudes* and Achilleas P. Achilleos†*
*University of Cyprus, Nicosia, Cyprus,
†Frederick University, Nicosia, Cyprus,
Email: {gkapi,adini-01}@cs.ucy.ac.cy, com.aa@frederick.ac.cy

***Abstract*—Many web and Internet of Things systems are based on user preferences and needs, in order to provide personalization. Such systems introduce privacy challenges due to the dramatic increase of data collection, whereas there is often a trade-off between the user privacy and the usability of the system. In the literature, various approaches have been followed to give users the possibility to define their privacy preferences. In this paper, we present an overview of different languages and techniques used for user privacy preferences modeling in different domains, along with systems that adopt these languages and consider users' privacy preferences. The approaches are categorized based on a taxonomy extended from a previous work, and their characteristics are compared. This study draws some conclusions on the adoption state of user-centric privacy management, whereas it aims to serve as an outline for further research efforts that are required towards an extensive implementation of privacy mechanisms in web environments, pervasive computing and the Internet of Things.**

***Index Terms*—privacy modeling, user privacy preferences, Internet of Things**

I. Introduction

Computing systems raise a wide range of privacy concerns due to the large amount of data that is collected about users for personalization or marketing purposes. The need for users to be aware and able to control which part of their data is shared has been identified in previous works [1]. The introduction of the EU General Data Protection Regulation (GDPR) has rendered this need more vital, as all applications need to comply with the GDPR principles. Privacy policies from the provider or the user side are usually employed as the means to describe what a service offers or what a user requires, whereas negotiation to consolidate the two sides and reach a mutual decision may also take place. Although users care about their data, in many cases they accept all requirements of the service provider regarding data collection, as they either need a large amount of time to understand the provider policies, or prefer the benefits gained from personalization in exchange for data privacy.

Having as motivation the above, in this work we are focusing on techniques that give users some level of control over the usage and distribution of their data. We present languages and modeling approaches that are used to express user preferences in terms of data privacy management, and we also take into account the mechanisms in place that consider these user preferences for the respective system adaptation. Previous works have surveyed security and privacy policy languages [2], [3], [4], but they are not focusing on the user end or are not investigating the relevant systems that adopt these modeling approaches to adapt the offered services. We consider the following domains of interest, since many works are tailored to a specific domain, although approaches from a specific domain may be applicable to another domain: web environment, pervasive computing, and Internet of Things (IoT), covering also generic approaches that do not fall into these categories.

The main contribution of our work lies in the consideration of the user side on privacy protection languages and adaptations. Our study can be a useful reference for understanding the current state, but also the existing challenges, as we provide a comparative view of existing works. We are not focusing only on formal security and privacy specifications (e.g. eXtensible Access Control Markup Language) that have been covered in previous surveys, e.g. [2], but investigate mainly more specific approaches that have been adopted in relevant contexts and can be potentially transferred to additional cases. We believe that this can be a useful reference for practitioners when they want to take decisions on how user privacy will be handled in their system, whereas it can trigger further research via the identification of open gaps in the provided solutions.

The rest of the paper is structured as follows. Section II gives a short overview of related work in the area, whereas section III introduces the methodology that was followed and the categorization of approaches used in our work. The next sections are dedicated to different domains. Approaches for the web are described in section IV, while section V presents approaches in pervasive computing. Approaches in IoT environments are detailed in section VI and general approaches are covered in section VII. A discussion follows in section VIII and finally, section IX concludes the paper.

II. Related work

The importance of data privacy vulnerabilities has been the subject of previous research works. Privacy risks that may exist in personalized systems are surveyed in [5]. The work focuses on social-based personalization, behavioral profiling, and location-based personalization. It discusses techniques that assist in reducing these risks, divided into pseudonymous personalization, client-side personalization, distribution, aggregation, perturbation and obfuscation techniques, privacy-preserving location tracking, whereas user controls and feed-

back are also indicated among the techniques. The focus of this work is on the risks and the relevant user side techniques that address the risks are presented very briefly.

An earlier work summarizes the available literature on privacy policy languages by listing available languages [2]. This work introduces the following features in the policy description: situation (e.g. capturing internal enterprise policies), representation (e.g. XML), evaluation (i.e. how decisions are taken), output schema, and implementation (e.g. type of application). Although it makes a categorization between enterprise and user policies, it does not discuss the role and the consideration of the user further.

The authors of [4] investigate whether privacy policy languages are adopted by users and data controllers investigating approaches for both ends (i.e. P3P, XPref, PPL, Rei, SecPAL4P, AIR, Jeeves, A-PPL and P2U), presenting the strengths and weaknesses of existing approaches. The main conclusions were that there is a lack of languages for normal web users, whereas for user languages a balance between the language expressiveness and the practicality of gathering required information from the users should exist. Languages that can be used in the semantic web are discussed in [6]. The following languages were compared using a number of scenarios: Protune, Rei, Ponder, Trust-X, KeyNote and P3P-APPEL. The work concluded that these languages cover many aspects well (e.g. access to private data) but more work is required regarding specifying minimal information disclosure and what happens to the data after disclosure.

The work closer to the current research work is a survey on security and policy languages [3] that builds on the work in [2]. This previous survey lists relevant security and privacy policy languages, introduces a multidimensional categorization, discusses open issues and emphasizes the need for negotiation and agreement specification. A more recent work discusses privacy policy languages in relation to existing legislation [7]. The authors identified 18 privacy policy languages but focused more on 4 of them (AAL/A-PPL, POL, PPL-XACML and QPDL) that fulfilled the criteria or describing system obligations and time constraints, and had a formalization. Laws and languages in smart city environments are surveyed in [8]. Languages used also in other domains are listed (P3P, APPEL, Rei, XPref, AIR, PPLS4P, Jeeves, A-PPL, P2P) and the characteristics of existing regulations are provided but the authors do not go into details for analyzing the language characteristics and usage. Seven previous works on smart cities are examined, but only two of them consider the user privacy preferences.

In comparison to previous works and especially [3] that shared similarities with our work, we do not discuss security policies or privacy policies from the provider side, but focus on the user end of privacy policies presenting approaches in different domains that can be a useful guide for researchers and practitioners in these specific domains. Moreover, we comment on the adaptation performed based on user privacy preferences, presenting existing systems that consider user preferences, an additional aspect that is not addressed in previous works but is necessary in order to understand the current adoption of modeling techniques.

III. Methodological approach

A. Collection of publications

In our study, we have collected a number of works from relevant conferences and journals. Our aim is to present approaches that put the user in the centre of the privacy preference specification and adapt to the user needs. Since this area is captured in conferences and journals that are not dedicated to security and privacy only, we used Scopus to search for publications covering any period till 2019 using specific relevant keywords that should be present in the paper as keywords or as words appearing in the title: 'privacy language', 'privacy modeling', 'user data privacy', 'privacy policy', 'privacy framework'. We did not use more generic search terms, as that would involve many irrelevant works and it would be practically impossible to examine them manually. For instance, Scopus returns 37,237 documents with the term 'privacy' in their title.

In this search process, we studied approaches that present mechanisms for privacy protection in the form of dedicated frameworks, as they usually include modules for user management. We are, however, not focusing on techniques for policy specification from the provider side, or for recommending user privacy settings. The papers included in this study satisfy one or both of the following requirements: i) provide a technique, language or model for users to specify their privacy preferences, ii) consider user privacy preferences in the system, application or service provision. Using the above approach, we collected papers, whose titles and abstracts were screened to examine if they satisfy the above requirements. Out of those, 53 had a relevant abstract and were selected to study their text. Publications that covered the service provider side or used formal techniques without discussing possible application in concrete systems, were rejected and the final number of publications that were considered is 30. Publications that appear in more than one searches or that refer to the same work were considered only once:

- *privacy language* - search result: 90, selection: 5
- *privacy modeling* - search result: 190, selection: 1
- *user data privacy* - search result: 174, selection: 5
- *privacy policy* - search result: 2,180, selection: 8
- *privacy framework* - search result: 1,018, selection: 11

B. Categorization of publications

In order to examine the characteristics of the privacy preference modeling, we adopt the categorization introduced for the case of policy languages in [3] and extend it with domain of use and maturity level, as shown in Fig. 1 in bold. The *domain of use* contains the applicable domain. Although pervasive computing and IoT have a close meaning, they are investigated separately, as not all approaches for pervasive computing are applicable also in IoT. The *maturity level* contains the following options:

- *Conceptual*: the modeling or language approach is conceptual and has not been implemented or used in a specific system.
- *Use case based*: the approach has been applied only in one or more specific use cases or scenarios.
- *Fully implemented*: the approach has been used in different contexts or in a wider system, usually in the framework of a research project, and has been the basis for adopting the offered services or applications to user privacy preferences.

Context sensitivity refers to whether the language allows to address variables of the environment in their rules and conditions. From this previous work, we are not depicting the *intention of use* property that is also part of the categorization (i.e. user requirements, enterprise policies, multiple policies interaction), as we are focusing only on the user (i.e. user requirements), and the type property (i.e. security, accountability, availability, privacy, data carriage, data usage control, network and device management), as we focus only on privacy and data usage control, and these elements are present in all of the approaches we consider.

Regarding application or service adaptation, we introduce the following properties that are visible in Fig. 2:

- *What part of the application or service is being adapted*: User Interface (UI) or application content are the most common adaptation cases, whereas the process of data collection, or the process of data sharing may also be adapted based on user preferences.
- *Means for user preference elicitation*: Information from the user only based on user preferences is used in most cases. Crowdsourcing techniques, or machine learning based (for recommending user privacy preferences) may also be utilized, whereas crowdsourcing is usually combined with machine learning. The crowd is not considered further in the current work and machine learning is found on a limited basis, as it is more relevant to recommendations of privacy settings.
- *Which additional information is considered in the adaptation*: Indicates whether data coming from other sources are considered. Context information with location being the most usual case can be encountered here.

We are not analyzing approaches for the social web further, as they do not propose new notations for specifying user preferences, but guide the users in making the most appropriate choices in the mechanisms already provided by the social network provider [9]. For the coding task, each author examined a number of papers and classified them based on the categorization. Another author verified the results, and discussions between all authors took place in cases of disagreement, until agreement was reached. In the next sections, the presentation of the approaches is performed based on the domain.

IV. Approaches for the web

Modeling. Among earlier approaches for the web, *APPEL (A P3P Preference Exchange Language)* allows users to express their privacy preferences as a list of rules [10]. This approach was targeting websites and has received critique, for example because it is hard to express simple preferences in APPEL. Some other works focused on the provider side, such as *P3P* that complements APPEL, whereas *XPref* is a XPath-based Preference Language for P3P [11]. APPEL and XPref have been adopted in order to allow patients to specify their privacy preferences on health-related data in a HIPPA (Health Insurance Portability and Accountability Act of 1996) compliant framework [12]. Motivated from P3P drawbacks, *SemPref* is semantics-based privacy preference language that contains accept rules and reject rules, with each rule consisting of a list of constraints [13]. Among those, data usage contains, for instance, the following elements: data, data-category, collection, purpose, purpose-required, recipient, recipient-required and retention.

The *eXtensible Access Control Markup Language (XACML)* is designed to capture Attribute-Based Access Control (ABAC) policies. The PRIME project has created *PPL (Primelife Policy Language)* as an extension to XACML with data handling and credential capabilities by defining a new obligation and authorization syntax [14]. *A-PPL* extends PPL to cover accountability needs [15]. A-PPL adds a number of constructs in PPL, and it defines the procedure for handling accountability, such as mechanisms for notification, logging and evidence collection.

In the area of e-Government services, users can define their preferences via a dedicated UI that is then translated in machine readable format in XML used to resolve conflicts with the policy of the service provider [16]. The user preferences contain the process, process type, storage, service provider and retention period. Sticky polices are used for the specification of privacy preferences of end-users, allowing to resolve conflicts that may exist between them and the privacy policies of the service provider in compliance to GDPR in [17]. The concept has been used in a proof of concept example application.

Modeling and system adaptation. In [18], context-based online privacy negotiation is used for handling private user information and users can define their preferences in a graphical user interface. A concept based on P3P elements (purpose, recipient, retention) is introduced. The proposed model depends on OWL (Web Ontology Language) representation of the P3P schema for the privacy domain to provide applicable alternatives for offers within a negotiation session.

PrivacySafer targets privacy protection in HTML5 web applications and allows users to define under which circumstances they wish to allow web applications to have access to their data, such as location, battery level, device orientation, accelerometer [19]. XACML is adopted and is extended for defining user privacy preferences, whereas JSON (JavaScript Object Notation) is used for implementation purposes. An abstract architecture is proposed for users' interaction with adaptive websites, enabling users to create and update their privacy preferences [20]. Users can create and keep their profiles (sets of information organized in one or multiple XML files) on the client side instead of the server side. This way the users are able to restrict the personalization experience

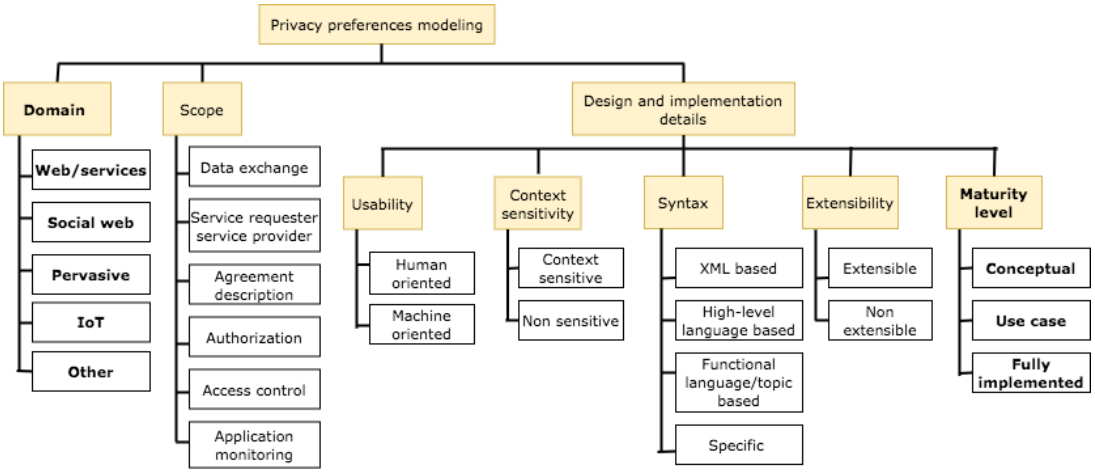

Fig. 1. Categorization of user privacy preferences modeling approaches ([3] extended)

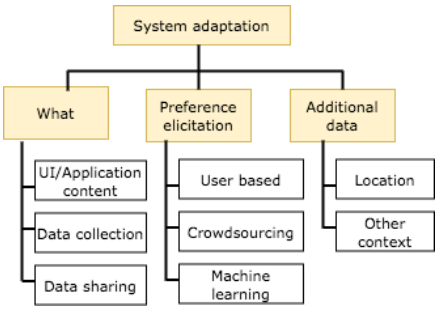

Fig. 2. Categorization of system adaptation approaches

these adaptive sites offer. The service provider builds the user profile by collaborating with the client in order to complete the personalization.

A privacy protection obfuscation mechanism for context-aware systems that meet the privacy preferences set by the users is described in [21]. The context model that is used to show the functionality of the obfuscation mechanism was built using the *Context Modeling Language (CML)*, where each object type in the context model is described with an ontology. Users control the obfuscation procedure by specifying their privacy preferences. The authors introduce also dynamic discovery and processing of context sources with rules.

In the field of web services, an approach that allows users to present their privacy preferences for adaptation in context-aware web service based applications is presented in [22]. The *Consumer Privacy Language (CPL)* includes a number of properties that are relevant to interactions with web services and enables users to define specific contextual conditions (e.g. specific times or locations) under which they allow or deny access to their data. XML notation is used for modeling.

V. Approaches in Pervasive Computing

Modeling. P3P terminology was adapted in [23] for the development of a privacy ontology for context-aware systems. A privacy rules class and relevant properties were defined to represent the users privacy preferences. Privacy rules are expressed in two classes, the data class and the condition class, and similar to the P3P specification the conditions can be classified based on various preferences, such as data recipient, data purpose, etc. The *Context-aware Privacy Policy Language (CPPL)* is a context-dependent privacy policy language for pervasive computing environments, where user's context is used as an additional condition for deciding upon granting or denying access to the requested resource [24]. CPPL defines privacy policies independently from the users' situation and considers social relationships to other users.

System adaptation. The *Secure Persona Exchange (SPE)* framework is based on P3P with an underlying notice-choice privacy model [25]. Personalization is provided through personas (user models) which are also used to represent user information. Machine-readable policies based on the P3P vocabulary are used to provide notice of data collection and decisions are based on user preferences expressed in APPEL.

Modeling and system adaptation. The *Discreet Privacy Language (DPL)* works along the Discreet Box, a privacy proxy that enforces privacy legislation principles [26]. The *SenTry language (SeT)* uses a user-centric privacy ontology on top of OWL and the Semantic Web Rules Language (SWRL) [27]. This way it allows the specification of fine-grained constraints on the use of personal and sensitive data to conform to the users' privacy criteria. Its enforcement point is the User-centric Privacy Framework (UCPF) that has been tested in the framework of a smart home laboratory.

In [28], an approach for building up user preferences that are not trusted in pervasive computing systems is being investigated. The underlying approach is based on creating a set of user preferences, captured in User *PPN (Privacy Policy Negotiation)* preferences, to assist in taking decisions relating to the selection of virtual identities, constricting them through the use of machine learning techniques. Textual rules are used for defining user preferences and are then transformed to XACML format. Jaroucheh et al. proposed a context information dissemination framework based on privacy policies for

pervasive systems [29]. They are using custom-defined XML schemas to model user privacy requirements. The system users can decide who is allowed to access their context information, such as location, at any given time.

P4P (Pervasive Platform for Privacy Preferences) is an extension of P3P that contains context-sensitive privacy control specifications [30]. Data elements in P3P specifications are represented by a tree structure. P4P is also a context-based negotiation framework that incorporates a context-aware policy design and personalization, by taking into account the user's profile as context. The users are allowed to negotiate according to their privacy preferences that can be specified in the provided user interface, where users answer questions, e.g. P4P using home address, P4P using phone number.

VI. Approaches in IoT

Modeling. A privacy preference model that allows users to specify how their data can be processed and what cannot be inferred from these data, along with mechanisms to enforce the preferences, are introduced in [31]. Data are part of specific categories, whereas the purpose of use is also indicated. User privacy preferences are composed of a tuple that contains an attribute of a data stream, the intended purposes for its collection and usage, an access constraint and the data categories not allowed to be derived from the attribute. The *Compact Privacy Policy Language (CPPL)* takes into consideration the need to have compact policies in the areas of IoT, cloud and big data [32]. It allows the users to define their policies regarding processing, routing and storage of data, in a human readable format, which is not further specified in the work, and it then compresses them to reduce their size.

System adaptation. Tailored to web-of-objects based smart home services, the *Smart Home Web of Object User Privacy (SWOPR)* architecture aims to control how user data are being released following user's consent [33]. The Privacy Controller (SWOPC) is responsible for collecting user data and preferences, whereas XACML is adopted for defining policies, but no further implementation details are provided.

Modeling and system adaptation. A privacy negotiation mechanism for IoT allows users to enforce their privacy preferences captured in XML format [34]. A negotiation protocol has been designed in order to model and realize privacy that covers the privacy requirements of all parties involved in an IoT interaction. The negotiation of the privacy policy is accomplished without any user intervention and supports the selection from multiple predefined privacy policies. The infrastructure developed with *Privacy Assistants* enables the discovery of nearby IoT resources (sensors, services, apps, device, etc.) and informs users about data practices associated with them [35]. The discovery of user-configurable settings for IoT resources is supported, enabling the privacy assistants to assist users to specify their privacy preferences. Machine learning techniques are used to build and refine models of users privacy preferences, so as to inform the users about data practices they are interested in and assist them in configuring the associated privacy settings.

Privacy Coach is an application running on mobile phones assisting users in making privacy decisions when confronted with RFID (Radio-frequency identification) tags [36]. This approach focuses on having the Privacy Coach acting as a medium between user privacy preferences and corporate privacy policies, attempting to find a match between the two and subsequently to inform the user. The user preferences are stored on the mobile device the first time the Privacy Coach is used and are requested via a question and answer wizard.

The *Semantic Web-based Context Management (SeCoMan)* framework for the development of context-aware smart applications provides users the possibility to define preferences for their location [37]. SeCoMan provides users the option of location cloaking (generates one or more fictitious positions), hiding their location to requesters, changing the granularity of their location using the levels defined in a relevant location ontology, and closeness specifies the minimum level of nearness the user wants to be located, whereas time can also be considered as a parameter in the user policies.

In the *PrivacyBat* framework, users can express their privacy preferences, when accessing nearby IoT devices via Bluetooth Low Energy (BLE) using the Privacy Preferences Expression GATT Service [38]. Users can specify a policy id, a relevant action and a policy preference. This is used in order to reach an agreement with the device. Devices then process user requests according to the agreement.

VII. Generic and other approaches

Modeling. A generic approach that can be used for personalized services, where users and applications negotiate data sharing is presented in [1]. The authors propose a policy framework for user data sharing across applications, the *Purpose-to-Use (P2U)*. A simple XML notation is used for specifying a user's policy. The negotiation process for data sharing and a respective compensation is offered to users. *SecPAL4P (SecPAL for Privacy)* is a generic language based on SecPAL that covers both the user and the provider side [39]. Users can specify how their personally identifiable information should be managed by services, whereas service providers can define policies about how they treat personally identifiable information collected from users. It introduces extended semantics in a specific syntax, but we have not encountered in the literature specific cases of its adoption.

Modeling and system adaptation. The *User-centric Privacy Framework (UPF)* aims to connect the legal language with the technical and the user language [40]. The system has built a dedicated UI for users, where they can choose among three predefined privacy levels (private, recommended, public) and a custom one, whereas a list of used levels is kept.

VIII. Comparison and discussion

The existing approaches are either generic or tailored to specific domains, although most belong to the second category. Some have been applied in specific scenarios, whereas others have remained only at conceptual level. In Table I, we show where each approach stands in relevance to the categorization

TABLE I
FITTING OF APPROACHES IN MODELING AND ADAPTATION CATEGORIZATIONS

Approach	Year	Privacy preferences modeling					System adaptation		
		Scope	Usability	Context sensitivity	Syntax	Maturity	What level	Preference	Additional data
Web/services									
PPL/A-PPL [14], [15]	2011, 2015	Data exchange, Agreement descr., Access contr.	Human	Sensitive	XML	Fully	Data collection, Data sharing	User based	Location, Other
e-Government [16]	2014	Data exchange	Both	Non sensitive	XML	Concept.	Data sharing	User based	n.a.
HIPAA-compl. [12]	2016	Data exchange, Access contr.	Human	Sensitive	XML.	Use case	App. content, Data sharing	User based	n.a.
[17]	2019	Agreement descr.	Human	Non sensitive	specific	Concept.	Data sharing	User based	n.a.
CML [21]	2005	Data exchange	Human	Sensitive	High level	Use case	Data sharing	User based	Location Other
[18]	2006	Data exchange	Human	Sensitive	XML	Fully	Data sharing	User based	Other
[20]	2008	Data exchange, Agreement descr.	Human	Sensitive	XML	Concept.	Data sharing	User based	n.a.
CPL [22]	2013	Authorization	Machine	Sensitive	XML	Use case	Data sharing	User based	Location Other
PrivacySafer [19]	2017	Data exchange, Authorization	Human	Sensitive	XML	Use case	App. content, Data collection	User based	Location, Other
Pervasive comp.									
[23]	2006	Data exchange	Machine	Sensitive	XML	Concept.	n.a.	n.a.	n.a.
CPPL [24]	2011	Data exchange	Human	Sensitive	XML	Fully	Data sharing	User based	Location Other
SPE [25]	2004	Data exchange	Machine	Sensitive	XML	Concept.	Data collection, Data sharing	User based	n.a.
SenTry [27]	2007	Data exchange	Human	Sensitive	XML	Use case	Data collection	User based	Location, Other
DPL [26]	2007	Data exchange	Machine	Sensitive	XML	Use case	Data sharing	User based	Location, Other
PPN [28]	2009	Data exchange	Machine	Sensitive	High-level XML	Fully	Data sharing	User based, Machine Learning	Location Other
P4P [30]	2010	Data exchange, Access contr.	Human	Sensitive	XML	Fully	Data sharing	User based	Other
infinitum [29]	2012	Data exchange	Human	Sensitive	XML	Fully	Data sharing	User based	Other
IoT									
[31]	2016	Data exchange	Machine	Non sensitive	High-level	Use case	Data collection, Data sharing	User based	n.a.
CPPL [32]	2016	Data exchange App. monitoring	Machine	Sensitive	High-level	Concept	n.a.	User based	Location Other
SWOPR [33]	2015	Data exchange	Machine	Sensitive	XML	Concept.	Data collection	User based	n.a.
Privacy Coach [36]	2010	Data exchange	Human	Non sensitive	High-level	Fully	Data sharing	User based	n.a.
SeCoMan [37]	2014	Authorization, Service req.	Machine	Sensitive	High-level	Use Case	App. Content	User based	Location, Other
[34]	2018	Data exchange,	Machine	Sensitive	n.a.	Fully	UI, Data collection	User based	n.a.
PPA [35]	2018	Data exchange	Human	Non sensitive	n.a.	Fully	Data collection	User based, Machine Learning	n.a.
PrivacyBat [38]	2018	Agreement descr.	Human	Non sensitive	High-level	Use case	Data sharing	User based	n.a.
Other									
SemPref [13]	2006	Data exchange	Machine	Non sensitive	specific	Concept.	Data collection, App. content	User based	n.a.
SecPAL4P [39]	2009	Data exchange	Human	Sensitive	specific	Concept.	Data sharing	User based	n.a.
P2U [1]	2014	Agreement descr.	Machine	Non sensitive	XML	Concept.	Data sharing	User based	n.a.
UPF [40]	2009	Data exchange	Machine	Non sensitive	specific	Use case	Data collection	User based	n.a.

presented earlier regarding privacy preferences modeling and system adaptation. *Extensibility* is not visible in the table, as all studied approaches are extensible. The indication 'n.a.' corresponds to cases, where the specific property is either not available or not relevant. Some more detailed properties regarding the mechanisms used in each approach are visible in Table II with an indication of the preference syntax, the specific domain or scenario used, and whether the service provider is considered either by expressing also provider policies or by offering a negotiation scheme between the provider and the user (or both). APPEL, XPref, and XACML are omitted from the table, as they have been covered at a large extent in previous works [4], [3].

Works in the IoT domain are, as expected, more recent. The recently enforced EU GDPR has been scarcely considered, since most approaches were conceived before its introduction and require adaptations in order to be GDPR compliant. Many approaches are based on existing standardizations, such as XACML, indicating a tendency to build on top of existing established languages. Generic XML is nevertheless, more usually employed. Although XML as a notation gives more flexibility, the problem arises from many independent ap-

proaches that are tailored to specific needs and cannot be easily generalized or deployed in different contexts, as the elements they contain are domain specific.

In the area of the web, some approaches consider the use of privacy policy languages, such as APPEL, for the specification of user privacy preferences, which is expected since such languages were developed for use in web systems. Nevertheless, these languages designed for the web are employed also in other areas, such as pervasive computing, since many systems are web-based also in this case. Table III contains summary information about the approaches we encountered. The categorization for the syntax of the policy modeling has been taken from [3], but in our work we did not encounter any approaches that used a functional language/logic based syntax. Nevertheless, examples of works with a logic based syntax exist but focus on the service provider side [41].

In terms of system adaptation to user preferences, most approaches modify the data collection or sharing to comply with user policies, whereas attempts that adapt the application content or user interface are few. Machine learning techniques for the system adaptation are less common and appear only in 2 of the studied approaches, as such techniques concern mostly approaches that provide recommendations for setting user privacy preferences. Such approaches were not further examined in the framework of the current survey. It is very positive that all approaches are extensible and almost all consider some form of context, both in the specification of user policies and the system adaptation, with user location being the most usual kind of data used.

Although there are approaches that provide recommendations to users on how they should set their privacy settings, more work is required toward this direction, as current systems are becoming more complex; making thus, policy specification equally complex for users. There is also a need for interoperability, since most of the approaches are autonomous and built for specific cases and may therefore, not be applicable in other cases. A major drawback is that most approaches do not offer intuitive user interfaces, where users can specify their preferences, whereas most do not offer any user interface.

Limitations. Our survey may have missed approaches that utilize existing privacy preferences models but do not express this explicitly in the paper title. Nevertheless, we believe that we have captured an important percentage of relevant approaches. Moreover, some approaches are immature and were not subsequently implemented or used in specific systems but we have listed them in order to provide an holistic view.

TABLE II
CHARACTERISTICS OF APPROACHES ON USER PRIVACY PREFERENCES

Approach	Specific domain of use	Specific syntax	Provider consideration/ negotiation
SemPref [13]	web	macro lang.	✗
PPL/A-PPL [14], [15]	cloud	XACML	✓
[16]	e-Government	XML	✗
[17]	online services	hard-coded	✓
[18]	e-commerce	P3P, OWL	✓
HIPAA-compl. [12]	e-health	APPEL, XPref	✓
CML [21]	pervasive	CML	✗
[20]	adaptive web sites	XML	✗
CPL [22]	web services	XML	✗
PrivacySafer [19]	web (HTML5)	XACML, JSON	✗
[23]	ubiquitous	ontology	✗
CPPL [24]	mobile	XML	✗
SPE [25]	ubiquitous	APPEL	✗
SenTry [27]	pervasive, smart home	OWL, SWRL	✗
DPL [26]	mobile	XML	✗
PPN [28]	pervasive, services	textual rule, XACML	✗
P4P [30]	e-commerce	P3P-enhanced	✓
infinitum [29]	pervasive	XML	✗
[31]	IoT	text	✗
CPPL [32]	IoT,cloud,bigdata	Boolean algebra	✗
SWOPR [33]	smart home	XACML	✓
PrivacyCoach [36]	IoT, RFID, mobile	n.a.	✗
SeCoMan [37]	IoT, smart apps.	text	✓
[34]	IoT, edge, cloud	n.a.	✓
PPA [35]	IoT	n.a.	✗
PrivacyBat [38]	IoT (BLE devices)	JSON	✓
P2U [1]	smartphone (scenario)	XML	✓
SecPAL4P [39]	any	text	✓
[40]	any	hard-coded	✗

TABLE III
SUMMARY OF LITERATURE REVIEW

Total number of approaches:	30
Number of publications with APPEL/XPref:	2
Number of publications with XACML adoption or extension:	5
Number of publications with custom XML:	7
Number of publications using ontologies/OWL:	3
Number of publications with other custom approaches:	13
Number of approaches funded by research project/grant:	12

IX. CONCLUSIONS

In this paper, we have presented an overview of approaches to user privacy preferences specification, focusing also on framework and system approaches that take these preferences into consideration for their adaptation. The common ground of all the studied approaches is that they consider that each individual user requires a different level of privacy preferences and application provision. This study can be a useful reference for the user guidance in the adoption of techniques for privacy preferences specification in different domains and also for revealing gaps that need further handling. Our current work focuses on the introduction of a consolidated model for user privacy preferences modeling specific to IoT systems, considering the heterogeneous nature of data collected in such environments, in conformance to GDPR. At the same time, we are focusing on adapting the service provision based on these user requirements in the context of an holistic user centric privacy framework in different scenarios including smart water management [42].

ACKNOWLEDGMENT

This work was partially funded by the Research Innovation Foundation of Cyprus RESTART 2016-2020 TAMIT (Novel Trustworthy Automatic Metering IoT Solution for Smart Cities Applications) project (grant agreement number ENTERPRISES/0618/0027).

REFERENCES

[1] J. Iyilade and J. Vassileva, "P2u: A privacy policy specification language for secondary data sharing and usage," in *Security and Privacy Workshops (SPW), 2014 IEEE*. IEEE, 2014, pp. 18–22.

[2] P. Kumaraguru, L. Cranor, J. Lobo, and S. Calo, "A survey of privacy policy languages," in *Workshop on Usable IT Security Management (USM 07): Proceedings of the 3rd Symposium on Usable Privacy and Security, ACM*, 2007.

[3] S. Kasem-Madani and M. Meier, "Security and privacy policy languages: a survey, categorization and gap identification," *arXiv preprint arXiv:1512.00201*, 2015.

[4] J. Zhao, R. Binns, M. Van Kleek, and N. Shadbolt, "Privacy languages: Are we there yet to enable user controls?" in *Proceedings of the 25th international conference companion on world wide web*. International World Wide Web Conferences Steering Committee, 2016, pp. 799–806.

[5] E. Toch, Y. Wang, and L. F. Cranor, "Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems," *User Modeling and User-Adapted Interaction*, vol. 22, no. 1-2, pp. 203–220, 2012.

[6] C. Duma, A. Herzog, and N. Shahmehri, "Privacy in the semantic web: What policy languages have to offer," in *Eighth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'07)*. IEEE, 2007, pp. 109–118.

[7] J. Leicht and M. Heisel, "A survey on privacy policy languages: Expressiveness concerning data protection regulations," in *2019 12th CMI Conference on Cybersecurity and Privacy (CMI)*. IEEE, 2019, pp. 1–6.

[8] D. E. Majdoubi and H. E. Bakkali, "A survey of major data privacy laws, languages and approaches in smart cities environments," in *Proceedings of the 4th International Conference on Smart City Applications*, 2019, pp. 1–8.

[9] K. D. Naini, I. S. Altingovde, R. Kawase, E. Herder, and C. Niederée, "Analyzing and predicting privacy settings in the social web," in *International Conference on User Modeling, Adaptation, and Personalization*. Springer, 2015, pp. 104–117.

[10] M. M. Lorrie Cranor, Marc Langheinrich, *A P3P Preference Exchange Language 1.0 (APPEL1.0)*, 2002. [Online]. Available: https://www.w3.org/TR/2002/WD-P3P-preferences-20020415/

[11] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "An xpath-based preference language for p3p," in *Proceedings of the 12th international conference on World Wide Web*. ACM, 2003, pp. 629–639.

[12] Y. Jung and M. Kim, "Hipaa-compliant privacy policy language for e-health applications," *Procedia Computer Science*, vol. 98, pp. 283–289, 2016.

[13] N. Li, T. Yu, and A. Anton, "A semantics based approach to privacy languages," *Computer Systems Science and Engineering*, vol. 21, no. 5, p. 339, 2006.

[14] S. Trabelsi, J. Sendor, and S. Reinicke, "Ppl: Primelife privacy policy engine," in *Policies for Distributed Systems and Networks (POLICY), 2011 IEEE International Symposium on*. IEEE, 2011, pp. 184–185.

[15] M. Azraoui, K. Elkhiyaoui, M. Önen, K. Bernsmed, A. S. De Oliveira, and J. Sendor, "A-ppl: an accountability policy language," in *Data privacy management, autonomous spontaneous security, and security assurance*. Springer, 2015, pp. 319–326.

[16] P. Drogkaris, A. Gritzalis, and C. Lambrinoudakis, "Empowering users to specify and manage their privacy preferences in e-government environments," in *International Conference on Electronic Government and the Information Systems Perspective*. Springer, 2014, pp. 237–245.

[17] N. G. Mohammadi, J. Leicht, N. Ulfat-Bunyadi, and M. Heisel, "Privacy policy specification framework for addressing end-users privacy requirements," in *International Conference on Trust and Privacy in Digital Business*. Springer, 2019, pp. 46–62.

[18] Y. He and D. N. Jutla, "Contextual e-negotiation for the handling of private data in e-commerce on a semantic web," in *System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on*, vol. 3. IEEE, 2006, pp. 62a–62a.

[19] G. M. Kapitsaki and T. Charalambous, "Adapting html5 web applications to user privacy preferences," *World Wide Web*, pp. 1–22, 2018.

[20] C. Kolias, V. Kolias, I. Anagnostopoulos, G. Kambourakis, and E. Kayafas, "Enhancing user privacy in adaptive web sites with client-side user profiles," in *Semantic Media Adaptation and Personalization, 2008. SMAP'08. Third International Workshop on*. IEEE, 2008, pp. 170–176.

[21] R. Wishart, K. Henricksen, and J. Indulska, "Context privacy and obfuscation supported by dynamic context source discovery and processing in a context management system," in *International Conference on Ubiquitous Intelligence and Computing*. Springer, 2007, pp. 929–940.

[22] G. M. Kapitsaki, "Consumer privacy enforcement in context-aware web services," *International Journal of Web Services Research (IJWSR)*, vol. 10, no. 3, pp. 24–41, 2013.

[23] N. Zhang and C. Todd, "Developing a privacy ontology for privacy control in context-aware systems," *Dept. of Electronic & Electrical Eng., Univ. College London*, 2006.

[24] A. Behrooz and A. Devlic, "A context-aware privacy policy language for controlling access to context information of mobile users," in *International Conference on Security and Privacy in Mobile Information and Communication Systems*. Springer, 2011, pp. 25–39.

[25] A. Brar and J. Kay, *Privacy and security in ubiquitous personalized applications*. School of Information Technologies, University of Sydney, 2004.

[26] G. V. Lioudakis, E. A. Koutsoloukas, N. L. Dellas, N. Tselikas, S. Kapellaki, G. N. Prezerakos, D. I. Kaklamani, and I. S. Venieris, "A middleware architecture for privacy protection," *Computer Networks*, vol. 51, no. 16, pp. 4679–4696, 2007.

[27] S. A. Bagüés, A. Zeidler, C. F. Valdivielso, and I. R. Matias, "Towards personal privacy control," in *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*. Springer, 2007, pp. 886–895.

[28] E. Papadopoulou, S. McBurney, N. Taylor, M. H. Williams, and Y. Abu, "User preferences to support privacy policy handling in pervasive/ubiquitous systems," *International Journal On Advances in Security Volume 2, Number 1, 2009*, 2009.

[29] Z. Jaroucheh, X. Liu, and S. Smith, "An approach to domain-based scalable context management architecture in pervasive environments," *Personal and Ubiquitous Computing*, vol. 16, no. 6, pp. 741–755, 2012.

[30] O. Kwon, "A pervasive p3p-based negotiation mechanism for privacy-aware pervasive e-commerce," *Decision Support Systems*, vol. 50, no. 1, pp. 213–221, 2010.

[31] B. Carminati, P. Colombo, E. Ferrari, and G. Sagirlar, "Enhancing user control on personal data usage in internet of things ecosystems," in *2016 IEEE International Conference on Services Computing (SCC)*. IEEE, 2016, pp. 291–298.

[32] M. Henze, J. Hiller, S. Schmerling, J. H. Ziegeldorf, and K. Wehrle, "Cppl: Compact privacy policy language," in *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society*, 2016, pp. 99–110.

[33] M. A. Latif, F. Ullah, H. Lee, W. Ryu, and S. Lee, "User privacy framework for web-of-objects based smart home services," *International Journal of Smart Home*, vol. 9, no. 5, pp. 61–72, 2015.

[34] K. Alanezi and S. Mishra, "A privacy negotiation mechanism for the internet of things," in *2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*. IEEE, 2018, pp. 512–519.

[35] A. Das, M. Degeling, D. Smullen, and N. Sadeh, "Personalized privacy assistants for the internet of things: Providing users with notice and choice," *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 35–46, jul 2018. [Online]. Available: https://doi.org/10.1109/mprv.2018.03367733

[36] G. Broenink, J.-H. Hoepman, C. v. Hof, R. Van Kranenburg, D. Smits, and T. Wisman, "The privacy coach: Supporting customer privacy in the internet of things," *arXiv preprint arXiv:1001.4459*, 2010.

[37] A. H. Celdrán, F. J. G. Clemente, M. G. Pérez, and G. M. Pérez, "Secoman: A semantic-aware policy framework for developing privacy-preserving and context-aware smart applications," *IEEE Systems Journal*, vol. 10, no. 3, pp. 1111–1124, 2014.

[38] S.-C. Cha, M.-S. Chuang, K.-H. Yeh, Z.-J. Huang, and C. Su, "A user-friendly privacy framework for users to achieve consents with nearby ble devices," *IEEE Access*, vol. 6, pp. 20 779–20 787, 2018.

[39] M. Y. Becker, A. Malkis, and L. Bussard, "A framework for privacy preferences and data-handling policies," *Microsoft Research Cambridge Technical Report, MSR-TR-2009-128*, 2009.

[40] V. M. Garcia-Barrios, "User-centric privacy framework: Integrating legal, technological and human aspects into user-adapting systems," in *2009 International Conference on Computational Science and Engineering*, vol. 3. IEEE, 2009, pp. 176–181.

[41] A. Gerl, N. Bennani, H. Kosch, and L. Brunie, "Lpl, towards a gdpr-compliant privacy language: Formal definition and usage," in *Transactions on Large-Scale Data-and Knowledge-Centered Systems XXXVII*. Springer, 2018, pp. 41–80.

[42] A. Dini Kounoudes, G. M. Kapitsaki, and M. Milis, "Towards considering user privacy preferences in smart water management," in *Adjunct Publication of the 27th Conference on User Modeling, Adaptation and Personalization*, 2019, pp. 209–212.