The Personalized Privacy Assistant for IoT Project

Lujo Bauer, Lorrie Cranor, Norman Sadeh, Anupam Das, Martin Degeling, Sruti Bhagavatula, William Melicher, Pardis Emami Naeini, Shikun Zhang

About the Project

We envision personalized privacy assistants as intelligent agents capable of learning the privacy preferences of their users and at times semi-automatically making many privacy decisions on their behalf.

This requires an infrastructure to communicate privacy policies between environments. We developed a machine readable privacy policy language for IoT and a web application for conveying the policy to users. Our IoT Assistant understands these policies and visualizes them in a mobile app.



Policy Language for IoT

Our policy language is implemented as a JSON Schema v4. It specifies necessary elements to describe IoT resources and services. It is both human and machine readable.

"contextType":{
"id": "#contextType",
"properties": {
"location": {
"description": "Where does data collection take place an "\$ref": "#/definitions/locationType"
},
"operator": {
"description": "What organization/individual owns and op "\$ref": "#/definitions/informationType"
}
"collector": {
"description":"What type of IoT device or system of dev: "\$ref": "#/definitions/collectorType"
},
"time": {
"description": "During which time period (day/week/month
"type": "array",
"items": {"\$ref": "#/definitions/timeType"}
},
"granularity": {
"description": "When the data is being collected, in what
"\$ref": "#/definitions/granularityType"
ſ
}, Urequiredu. [Uce]]ecteru]
"required": ["collector"]

nd who is responsible for that", perates the devices?",

ices are collecting data?",

etc) does data collection take place?",

t form is it collected?",

IoT Resource Registry

Web application that can be set up in any loT environment.

Those responsible for setting up IoT devices can register their resource, specify what the data is collected, how data is processed, how long data is stored and which control choices (REST APIs) are available to users.

The IRR is advertised with Bluetooth beacons that can be discovered by the IoTA.

The IRR is build on the open MEAN Platform (Mor and allows authentication with any OAuth provider.

<u>≙</u>	* 💎 🖹 🗎 1:0	8 🖬 🗳	* 💎 🖹 1:08	The Ir
IoTAssistant	:]		discov
RESOURCE	SERVICE		7]]]	the pr
	IoT Resource			use int
Tippers Presence Sensor))))	Wifi and Bluethoot	h based Location Sensing	
Wifi and Bluethooth based Location Sensi	ng	COLLECTOR		llcorc
OPTIONS		Collector Description	Wifi and Bluethooth based Location Sensing	Users and s
		LOCATION		
Wean Location Tracker	IoT Resource	Location Name	Donald Bren Hall	service
Presence Sensor Wifi and Bluethooth based Location Sensi	1 '''	Location Owner Name	UC Irvine	availab
		OPERATOR		other \
OPTIONS		Operator Name	Information Systems Group	
		RETENTION		
Video Obfuscation Camera Video Cameras	IoT Resource		SETTINGS ation tracking is enabled on tracking is enabled	In the users'
		\triangleleft	0	semi-a

Acknowledgement

Our research is generously supported by









Carnegie Nelon University www.privacvassistant.c

xes ← IoT Services ←			2	-
Iot Re	esource Reg	gistry		
IoT Resources IoT Services			2	
F	Register a new IoT Res	source		
■ Basic Information Context	ed : :: Granularity ? Purpose	O Times and Retention	With O	Control ptions BMIT
Collected Data				
Collecting Device That type of IoT device or system of devices are collecting data? Collecting Device* UIFI Location Tracker MAC	iption Adresses are collected to allow location sharing	Link to additional infor https://	mation	
ypes of Data				
escribe the type of data inits connections per second	Value 10			

nternet of Things Assistant (IoTA) vers IRRs via Bluetooth and renders rivacy policy language in an easy to erface.

can learn about nearby resources services, download and use the es. The IoTA emphasizes the choices ble (like opting out or in or choose variants of data collection).

future the IoTA will be able to learn preferences and apply them utomatically.