



UNIVERSIDAD DE GRANADA

Living in a Smart Global Village: a Data Collection Story

Daniela Popescul, Alexandru Ioan Cuza University, Iasi, Romania - rdaniela@uaic.ro

Background

- nowadays, our lives are recorded by various new companions as smart wearables (e.g. watches, bracelets, glasses, clothes), smart appliances (e.g. refrigerators, robotic vacuum cleaners, TV sets or coffee filters), and not only in our homes and offices, but also in auto and pedestrian traffic - by smart cars, buses and even smart streets
- this perpetual collection of people’s data enables one to track the actions and behavior of the users and derive sensitive information about individuals, which is not only utilized by the technology itself but also by third parties such as businesses, hackers and governments

Aim

- to increase readers’ awareness by presenting an exhaustive inventory of data being collected, stored and processed in a smart environment

Methodology

- a set of ten privacy policies published by selected manufacturers of smart watches, health and fitness trackers, smart TVs and smart cars were overviewed
- the main data categories collected by the manufacturers were extracted and sorted, in order to get an image about the extent of our lives being recorded while using such devices

Results

Data collected by Smart TVs

	Panasonic	Samsung	Sony	Philips
Identification data				
Name	*	*	*	
Username & password		*		* (consumer ID)
Email address	*	*	*	
Profile picture	*			
Phone number	*	*		
Postal address	*	*	*	
Payment information (credit/ debit card)		*	*	
Age/ date of birth	*	*	*	
Gender	*	*		
Location				
Postcode				
Physical location of the device (GPS)	*	* (if consented)	*	
Nearby Wi-Fi access point	*	*		
User generated data				
Photos		*	*	
Texts		*	*	
Calendar		*		
Contacts		*		
Device data				
Device model	*	*		
Device serial number	*	*	*	
Date of purchase	*			
Operating system version	*	*		
Configurations and settings	*	*		*
MAC & IP address	*	*		*
Channel zap behaviour				*
Time and date of a “click” in the menu				*
Automatically collected data (service use)				
Log files, search queries	*	*		
Time and duration of use	*	*		
Cookies	*			
Applications installed				
Application click behaviour		*		*
Browsing data	*	*		*
Used online applications	*			
Voice recordings (voice commands to a service)	*	*		
Messages on discussion boards	*			

Data collected by smart watches and trackers

	Vector	Huawei	Apple	Samsung	Fitbit
Identification data					
Name		*		*	*
Username & password	*				*
Email address	*	*		*	*
Profile picture		*			*
Phone number	*	*		*	*
Postal address	*			*	*
Payment information	*			*	🔒
Age/ date of birth	*	*			*
Gender, height, weight	*				*
Biography					*
Location					
Country information					*
Real time location	*	*		*	*
ID of area where the device is located/ approximate location		*	*		
User generated data					
Photos	*		*		
Texts	*		*		
Calendar			*		
Feedback	*				
Data about purchased products		*			
E-mails			🔒		
Used apps			*	*	
Visited websites				*	
Number of steps, calories burned, distance travelled, sleep stages					*
Contacts’ data					
Name, profile picture, phone number and email address		*	*		*
Email addresses, social networking accounts, contact list on mobile device					*
Automatically collected data (service use)					
Log files, buttons pressed	*				
Support requests and results	*				
Search queries	*	*		*	
Streams and apps downloaded and stored	*		*		
Device data					
Model	*			*	
ID/ name	*	*	*	*	
Serial number	*	*	*	*	
System and application versions		*	*	*	
Regional and language settings		*		*	
Time/ duration of use			*	*	
Additional data					
Voice information recordings (shared with 3 rd parties)				*	
Female health tracking					*
Messages to friends on discussion boards					*
Communication with coach					*

Discussion and conclusions

- we do not express doubts about the declared purposes of data use in the policies, which refer mainly to service provision, product and services development, marketing, security assurance, fraud prevention and investigation
- we just intent to signal the fact that the extended use of IoT by citizens creates an extended attack surface for potential hackers, as big as our daily life
- besides the probability of attacks, other problems can be signaled: the process of collecting data is not transparent for the average user, the entities that use the data are often unknown and use inconsistent security measures, the privacy settings are buried deep in Settings menus, being difficult to be found and modified; when disabled, the “smart” functionalities of an object are reduced and valuable features are lost
- data flows function as serotonin intakes, offering us the illusion of happiness. But, on the other side of the story, same flows form quasi-permanent digital traces with unexpected uses – as mass aggregation in marketing databases, invasive target advertising, with effects like loss of autonomy and individual freedom

Organizan



Financian



BOULEVARD • Aragón • Asturias • Cantabria • Castilla-La Mancha • Castilla y León • Cataluña • Extremadura • Madrid • Murcia • Navarra • País Vasco • Rioja • Valencia • Galicia • Asturias • Cantabria • Castilla-La Mancha • Castilla y León • Cataluña • Extremadura • Madrid • Murcia • Navarra • País Vasco • Rioja • Valencia • Galicia