To be filled out in the EDPS' office

REGISTER NUMBER: 900

NOTIFICATION FOR PRIOR CHECKING

Date of submission: 25/09/2012

Case number: 2012-0824

Institution:European Commission

Legal basis:

Article 27.2.(a) Processing of data relating to health and to suspected offenses, offenses, criminal convictions or security measures

Article 27.1 Other (general concept)(1)

(1) OJ L 8, 12.01.2001

INFORMATION TO BE GIVEN*(2)*

(2) Please attach all necessary backup documents

1/Name of the processing

Participatory surveillance research project with evacuation exercise at □
JRC/IPSC Institute

2/Description

during an evacuation exercise. Participatory surveillance is a novel approach that relies on sensor data from smartphones to contribute to surveillance tasks (e.g. location tracking, identity verification, etc.).
The processing consists of capturing and remote recording smartphone sensor data (location, video, sound, etc.). The identification component processes as well participant identification data (name, surname, ID, building, office and photo) to produce badges and perform id checks on mobile devices at the meeting point.

According to privacy-by-design and data protection principles (proportionality, duration, consent, non disclosure to other parties, data minimization and anonymization/aggregation of the presented results), we developed and implemented a participatory surveillance testbed. Software and mobile devices (i.e. a dedicated application, 12 smartphones and 100 contactless identity cards) will be distributed to a group of volunteer employees with different roles (building delegate, end user) at one of the JRC yearly evacuation exercise (bld. 36).

The experiment will focus on evaluating the technological dimensions of participatory surveillance and might also contribute to enhance the JRC local emergency procedures (cfr. document on standard operative instructions of building delegate tasks) as follows:

1. Preparatory registration

The control room maintains a list of mobile phones assigned to users who will participate to surveillance with their devices providing various sensing capabilities. The participatory surveillance software is installed in each mobile phone and ready to be used by the building delegate as authenticated user or staff member as simple end user. The control room also maintains the list of staff to be evacuated (i.e. the persons who received the duplicate identity badge required for the participatory surveillance test).

2. Participatory surveillance services for evacuation monitoring

The evacuation alarm will constitute the starting point of the participatory surveillance test and will notify to the user the need for activating the corresponding software on the smartphones, enabling the following services.

2.1 Automatic location tracking

The location of smartphones involved in the test will be continuously transmitted to the control room and displayed on the map of the evacuation premises (indoor and outdoor area). Additionally the building delegate contact details will also appear on the map. This function will be available only during the exercise.

2.2 Manual video streaming

Either on request from the control room or on their own initiative, building delegates will be able to stream short sequences of audio/video content reporting critical events in real-time to the control room.

Throughout all the evacuation procedures, smartphones will capture relevant contextual information that will be uploaded to the control room repository and eventually analysed (speed, battery level, etc.).

2.4 Biometric identity verification of staff members at the meeting point

During the final stage, the building delegate will use the smartphone as contactless card reader to verif the identity of the people present at the meeting point cross-checking it against the evacuation list. The basic mechanism for the authentication will be face recognition, the user presents his badge to the building delegate smartphone and then the picture read is matched against the one taken on the spot. The procedure ends with the building delegate sending either an “OK” or the list of missing employees to the control room.

As backup solution (e.g. badge left in office), the identity matching could also be performed remotely on the control room server. Only a couple of pre-selected users (no more than 10) who would have provided consent to this back-up solution will contribute to this part of the test.

3. End of evacuation exercise

Having received the result of the presence check, the control room can notify the correct execution and conclusion of the exercise. This notification will stop all data collection and finalise their uploading of the server.

4. Post-analysis reporting

The personal data collected in raw format during the exercise will be analysed and aggregated into anonymous statistics (e.g. duration, location, activity). Personal data on badges and smartphones will be deleted after the exercise execution.

3/Processors

Not applicable.

4/Automated / Manual operations

□

User data encoding on badge and mobile identity verification.□

Automatic sensor data capture running in background on mobile devices and □ storage on server.□

Video recording on smartphone memory card and server repository (video □ content could be reused for scientific/research publication with granted □ permission from data subjects. Face will be blurred on the video used for □ those publication).□

Data quality assessment.

5/Storage

Collected data will be kept on direct access storage of the Digital Citizen □ Security unit lab server, physically disconnected from JRC Internet and not □ accessible from outside world. From enrolment to evacuation execution, □ identification data will also be encoded on badges and backed-up on server.

6/Comments

□
Identity authentication is performed as a “one to one” match between data □
read from the badge and captured by the smartphone. As back-up solution □
(e.g. some participants will simulate the loss of their badge), □
verification is performed on the server by matching the person photo □
against the volunteer database.□
The software is developed reusing and testing as many as possible □
innovative tools and applications available for android devices.□
Biometrics: Megamatcher embedded SDK by Neurotechnology, additional tests □
of android.media.FaceDetector library for face recognition, Eigenfaces □
algorithm based on PCA.□
NFC: ISO 14443/A proximity communication standard, MIFARE Desfire (8K)□
Sensor data collection: Funf open sensing framework developed by the MIT □
available online at http://code.google.com/p/funf-open-sensing-framework/□
Location tracking: inhouse developed component□
Video streaming: component assembled from android applications (SpyDroid, □
IPWebCam, Xuggler).

7/Purposes

The purpose of the processing is to study feasibility of the participatory □
surveillance concept and its legal and technical issues when using latest □
generation smart mobile devices (smartphones, duplicates of contactless □
identity cards) such as privacy opt-in/opt-out choices, reliability, □
efficiency and scalability of the exercise.

8/Legal basis and Lawfulness

□
Framework 7 Research Programme under which the JRC provides technical and □
scientific support to EC policy development: COUNCIL DECISION of 19 □
December 2006 concerning the Specific Programme to be carried out by means □
of direct actions by the Joint Research Centre under the Seventh Framework □
Programme of the European Community for research, technological development □
and demonstration activities (2006/975/EC) (2007 to 2013)□
□
The processing of personal data is lawful following Art. 5.a and Art 5.d: □
the data collection of building delegates and end users is organised on a □
voluntary basis and the transfer of data of building delegates is performed □
only with their explicit consent.

9/Data subjects

* Building delegates (1 to 2)□
* Staff employees from IPSC bld. 36 and enrolled for the participatory□
  surveillance project with a smart phone provided to them (10) or with□
  their own smart phone (min 20)□
* Staff employees from IPSC bld. 36 and enrolled for the participatory□
  surveillance project with a dedicated badge produced for the□
  test.(max 100)

10/Data fields / Category

□ Biometric/personal data for badges (identifier, name, surname, identity □ photo, office, building)□ □ Smartphone user data: (android version, battery status, smartphone model, □ network unique identifier, installed & running applications, audio, light, □ proximity, magnetic field, raw and derived accelerometer values, gravity, □ orientation, GPS/network location, nearby bluetooth & WiFi devices), □ including short sequences of video-streams can include images of objects, □ cars, and individuals.
11/Mandatory Information □ At recruitment data subjects will be informed of all experiment terms by a □ privacy statement, participation is only on voluntary basis.□ □ 100 badges and 12 smartphones will be configured and distributed to □ volunteers (building delegates and end users).□ □ The participatory surveillance software limited to the sensor data □ collection component (a modified version of the open source Funf software □ made available by MIT at □ http://code.google.com/p/funf-open-sensing-framework/□ <http://code.google.com/p/funf-open-sensing-framework/>) will also be □ distributed to voluntary users wishing to use their personal smartphone at □ the exercise and consenting to be followed along the evacuation stages.
12/Procedure to grant rights Data subject will be offered the opportunity to correct and modify the data □ they provided and to withdraw their participation at any time by contacting □ the contact point of the project (a dedicated email and phone number will □ be available for this point).
13/Retention □ Biometric and personal data encoded for badge production will be retained □ for the time necessary to conduct the experiment and will be deleted within □ 30 days after the evacuation test.□ □ Smartphone user data and short sequences of video streams will be retained □ in raw format for the time necessary to perform post-analysis evaluation □ and technique validation of location tracking, quality assessment of video □ content (1 year).
14/Time limit Should any data subject withdraw their consent on the use of collected □ data, request modification will be made within one month.
15/Historical purposes Only anonymous statistical data.
16/Recipients

□
No personal data is transmitted to third parties, which are outside the □
recipients (IPSC SURCIT researchers) and the legal framework mentioned.□
□
The access to all personal data is only granted through User_Id / Password □
to a defined population of users. These users typically are: the Unit Head □
acting as controller of the processing of personal data, the system □
administrator of the software and the unit staff members from the SURCIT □
action involved in the research project. Regular registered and approved □
users by default have access to limited personal data of other users: □
username, location, occupation, and signature. □
□
Experiment results will be made available to IPSC/ISM safety and security □
unit only in the form of anonymised and aggregated data. The data related □
to the building delegate who is an important actor of the traditional □
evacuation exercise will be transferred to the safety and security unit □
only with his explicit consent.

17/Transfer out of UE/EEA

Not applicable

19/Complementary information

PLACE AND DATE:25/09/2012

DATA PROTECTION OFFICER: MANOLESCU Dan

INSTITUTION OR BODY:European Commission