On the Successful Deployment of Community Policing Services the TRILLION project case

Charalampos Z. Patrikakis, Dimitrios G. Kogias

Piraeus University of Applied Sciences

Egaleo, Greece

George Loukas, Avgoustinos Filippoupolitis, William Oliff, Syed Sadiqur Rahman

Computing and Information Systems

University of Greenwich, UK

Silvio Sorace, Ernesto La Mattina, Quercia Elisabeth

Engineering Ingegneria Informatica SPA

Italy

***Abstract*—The evolution of policing towards the next generation, not only involves confronting new types of crime such as cybercrime, but also the active engagement of citizens in the process of creating a secure environment through the deployment of community policing practices. However, in order to fully exploit the potential of community policing, the building of trust between citizens and Law Enforcement Officers is important. In this paper, the authors (all participating in the EU Research project on community policing TRILLION), discuss issues related to the use of innovative technologies, while ensuring societal approval, in the context of community policing. Both requirements and corresponding work leading to the actual implementation of a fully operational platform are presented.**

Keywords—community policing, privacy protection, mobile devices, wearables, serious games

I. INTRODUCTION

Community policing has evolved into the preeminent reform goal in modern policing, which differs from traditional policing via a shift towards more citizen involvement, geographic focus, more opportunities for interaction with citizens, and an emphasis on prevention [1, 2]. Naturally, this approach puts considerable pressure at organizational level, for moving from a top-down approach of police management to a bottom-up approach, where citizens have a more active role. Another key challenge relates to trust issues within and between the law enforcement agencies and the citizens. Motivation for engaging citizens in this community driven policing framework is also crucial. Community policing has been used successfully in crime reduction [3], extremism prevention [4], and even in counter terrorism [5]. All these cases were based on direct face-to-face or over-the-phone interaction between the community and Law Enforcement Agencies (LEAs). There is a growing realization that technology has the potential to accelerate the evolution towards more effective community policing [6].

In particular, social media is one type of technology that has been used by LEAs worldwide. In [7], the authors investigate the use of Twitter by Dutch police officers. The study highlights that the use of social media reduces organisational boundaries and stimulates internal and external communications. An analysis of Twitter adoption among municipal police departments in the U.S. in cities with population larger than 100,000 [8] indicates that there are regional factors that affect speed of adoption, while organisation size does not to play a significant role. The use of Facebook by the Bangalore City Police is described in [9], where the authors conclude that social networks can be used by the police to obtain actionable information (e.g., crime location and evidence) from residents.

Another popular type of technology being used by LEAs is purpose-built software tools. A mobile application for community policing, which supports continuous video recording and event capturing, is presented in [10]. The authors, who evaluated the tool via a questionnaire, concluded that the main motivation for users' participation was traffic safety promotion, while the use of the tool results in promoting safety awareness. Another mobile application geared towards gunshot detection is described in [11]. By using mobile phone sensors, the application can detect between fast and slow gunshots, and can help determine whether the shot was fired by the mobile phone user or by someone nearby.

EU H2020 project TRILLION takes the concept of technology-assisted community policing further and is currently developing a community policing platform, which aims to contribute to a safer society, encouraging interactive partnerships between law enforcement officers and the people they serve, implemented over an open, flexible, secure and resilient socio-technical set of tools. Citizens will be able to report crimes, suspicious behavior and incidents, identify hazards and assist law enforcement agents actively. As a result, LEAs will be able to detect incidents in a more efficient, content and context aware manner, locate onsite citizens, other LEA representatives and first responders communicate with them, request further information and assign them specific actions to address on-going incidents.

'TRILLION primary challenge is to facilitate effective cooperation between citizens and law enforcement agencies as well as between citizens through bi-directional communication.

Feedback and service are also important, as well as taking information security and personal integrity into consideration, while being personal enough to motivate people to use the system. Requirements for TRILLION include building trust and confidence for the police as well as within the agency and facilitate communication and cooperation among citizens and between law enforcement agencies and citizens.

To establish a reliable scenario framework, TRILLION has adopted the methodology proposed by RAND [12-13], which is based on the observation that the most important factors driving the future of law enforcement fall into two categories: Technology and Society. The effectiveness of the technology used by LEAs in supporting their mission depends on the level of the technology itself (vertical axis, increasing from bottom to top) and the extent to which law enforcement practices are accepted by society (horizontal axis, increasing from left to right). As presented in Figure 1, the quadrant is delimited by technology and society axis, creating four different situations/futures.

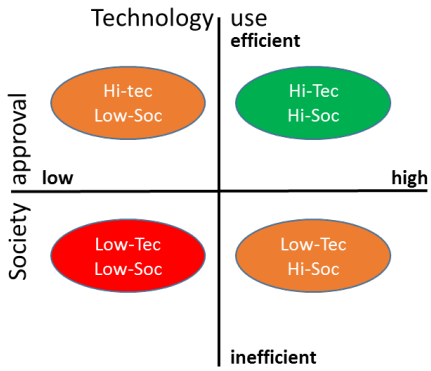

Figure 1: Use of technology and societal approval (RAND quadrants)

The description of each scenario quadrant is as follows:

a) **Hi-Tec/Hi-Soc**: The upper right corner represents a situation/future where LEAs use advanced technology for dealing with different situations. At the same time, LEAs enjoy societal support concerning the actions taken to protect the public.

b) **Low-Tec/Hi-Soc**: The lower right corner represents a situation/future where LEAs use obsolete technologies, but the society continues to support their efforts for protecting the public.

c) **Hi-Tec/Low-Soc**: The upper left corner represents a situation, in which LEAs have the advantage in the use of technology, but have lost the society's trust, which strongly opposes every action they take.

d) **Low-Tec/Low-Soc**: The lower left corner represents the most challenging situation/future, where LEAs use old technologies and have to face a society which strongly opposes every LEA measure and action.

As TRILLION introduces several technologies for community policing, it is obvious that its success depends on the adoption of the technology and its societal approval, as represented in the Hi-tec/Hi-Soc top right quadrant, where Citizens and LEAs work together and fully utilize current technologies. This paper focuses on four directly related aspects of the design and implementation of TRILLION's platform:

1. Usability of tools and applications for reporting and communication of incidents,
2. Information and system trustworthiness, which is important for building trust over credible and certified information,
3. Protection of privacy, supporting even "anonymous" reporting, which has proven very effective in fighting organized crime in certain conditions [14-17], and
4. Training on the use of the new tools.

In the rest of the paper, we first present the requirements for each of these four aspects (Section II) and continue with their practical implementation in TRILLION (Section III). These include technologies for mobile and wearable devices, as well as the use of a serious gaming approach to support community policing and to raise awareness respectively. The aim is to achieve:

a) **efficient use of existing technology** in order to guarantee *trustworthiness of information*, and *effective training* which will in turn increase the likelihood of correct use of the TRILLION tools and services,

b) **high societal approval**, through the guarantee of *protection of personal data* while ensuring the *usability of the deployed tools*, so that they are easy to master, memorise and use, enabling citizens to quickly and accurately report and respond to safety related incidents.

By successfully addressing the four topics related to technology use and societal approval, the final result is expected to be placed on the top right quadrant of the RAND model.

II. Requirements for Community Policing Platform

A. Usability

Usability is an important non-functional requirement for a community policing platform. To be easy to learn and support speed of communication, its end user applications should feature a simple User Interface (UI), allowing users to quickly select, annotate and submit incident reports, incorporating multimedia content captured over their mobile or even wearable devices. To reach this goal, the design of the applications must abide by well-documented usability guidelines regarding the size and place of interface items (for example the OK button should be placed on the bottom left corner while the CANCEL button on the bottom right one) along with the right selection of colors to enhance the user experience.

The ultimate goal for the end user applications is to offer the tools for reporting of incidents, allowing for completion of the reports in a very short timeframe, avoiding delays in the communication with the platform or during the process of creating the report.

Since content (e.g., audio or video) documenting the reported incidents is important, another challenge is the effective handling of this content, ensuring rapid transmission and subsequent removal from the end user's device. The aim is that reports created by users will not have any effect to the use of their personal devices (such as use storage space for the multimedia files accompanying the report) and will also avoid the risk of putting the users in any dangerous situation (if their devices fall in the hands of people involved in the reported incident).

Finally, the user should be able to interact with the system both via apps on mobile and wearables devices, and conventional desktop computing, which creates the need for a particular design of UI, which is appropriate on all these platforms. Given the enhanced capabilities that mobile and wearable devices have for situation awareness, it is important that these capabilities are taken advantage of, allowing for example an elderly person to use a smart watch to make a certain gesture that will raise an alarm or send a distress signal.

B. Trustworthiness of information

The reliability of the produced reports is very important, since any further actions such as communication with the authorities, issuing of warning, or calls for assistance will depend on it. Here, the focus is on cyber trustworthiness, which can be defined as the likelihood that a report has not been maliciously modified or delayed via cyber means [17]. Producing a cyber trustworthiness score for each device used in creating a report requires (a) monitoring the required data sources, (b) evaluating the likelihood of the device having been maliciously manipulated, and (c) displaying it to the device's user. Correspondingly, the first key requirement is to provide access to a large number of data sources related to trustworthiness on the mobile device without requiring for it to be jailbroken. These data sources range from different aspects of memory, network and processing usage, to current, battery consumption and mobile and GPS signal strengths. In practice, certain permissions need to granted to expose some of these data sources to the application. A related requirement is to allow logging the data samples that have collected, thus allowing for large volumes of data to be stored without the issue of requiring a large segment of memory. Logging the data samples also provides the benefit of creating historic data, which can be used in future analysis in attempt to identify tends in the data. These trends can then be used to further enhance the cyber trustworthiness monitoring when determining whether the device is exhibiting abnormal behaviour or usage. Furthermore, as the data is logged in the mobile device's non-volatile storage, the collected data would not be lost if the device were to suddenly lose power (e.g., when the battery is depleted). If a power failure were to occur, the application would simply need to reopen the file again once power is restored. The second key requirement is that the cyber trustworthiness mechanism produces a dependable score that exhibits high accuracy against the ground truth in a variety of normal use and malicious manipulation scenarios. The third key requirement is that the user is informed in near real-time of the cyber trustworthiness score of the device with a visualisation approach that does not interfere with normal use.

C. Privacy Protection

A lot of work has been carried out in identifying ethical and privacy issues related to the use of computer applications, resulting to a specialization of particular areas which could be affected, such as workplace privacy, medical privacy, genetic privacy [18], and Internet/public privacy [19].

To encourage the use of the system, the user should be allowed to select not only the platform for the communication but also the shared information that will be needed. For example, when a photo from a certain event used in a report, then the faces of the people participating must be blurred to avoid any unwanted exposure to the public. Consider the case of a car accident and a photo of the incident uploaded in a report containing the faces of the passengers and the people nearby that have not been informed. One of the most important features of the privacy protection is that users should be able to submit a report without having to reveal their identities, at least not without consent. At the same time, certain information should be provided to deter someone from reporting a false incident on purpose.

D. Training on the use and mastering the platform

Any perceived lack of trust between citizens and LEAs can negatively affect collaboration between them. Indeed, the social capital is central to enable partnerships and help communities in finding solutions to problems through collaborative problem solving. In this context, using serious games is a very attractive mechanism for engaging citizens and growing their awareness with respect to location, communication and interaction awareness:

- *Short Term Awareness*: Location awareness. The gaming setting (objectives, virtual characters, storytelling, etc.) should empower spatial and location knowledge (be aware of the surrounding environment). This can help in informing citizens about critical locations (dangerous areas, important behaviors to be promoted in places, etc.) or the location where they can seek assistance.
- *Mid Term Awareness*: Communication awareness. This setting enables virtual and controlled communication with virtual characters. The aim here is to maximize the efficiency of communication between officers and citizens. Virtual stories recreate plausible storylines during which the user has to show a set of correct behaviors.
- *Long Term Awareness*: Interaction awareness. This setting is created in order to improve the awareness of citizens about potential scenarios of real cooperation with LEAs, thus improving their operational skills in critical situations (e.g., first aid).

Serious games can play an important role in transforming LEA-Citizen relationship for the better. In this space, utilizing the mobile platform makes sense. Mobile technologies have evolved

rapidly over the last decade, and importantly are accessible by the vast majority of the population.

The question is which platform can be used to play a serious game and to reach the largest audience. In the last decades, mobile technologies have quickly shifted computation and data communication from computers to smartphones and tablets. For raising awareness to citizens via serious games, they offer two key advantages: They are already equipped with many sensors useful for serious games (players do not need to buy new devices), and equally importantly, the simulation of events and conditions can be carried out by devices and systems that the players/citizens already use for similar purposes in their life. Both of these advantages contribute considerably in moving from the bottom to the top of the RAND chart (efficient and effective use of technology).

III. PLATFORM

In this section, we will present the implemented TRILLION platform, following the recommendations given above.

A. Usability

Considering the aforementioned usability requirements and feedback received during a mockup validation process, the end user applications were designed to be simple and easy to use, especially as regards the generation and submission of a report.

A user can create and send a new report in just three steps, following the instructions provided in each one. In the first step (s)he can choose from a list the category of the report, and select the report's location. In the next step, a small description is required, and optionally the user can also attach media files such as image, audio or video, either preexisting or new using the devices' sensors (camera, microphone). In the final step, the user can review the report to be sent, modify, if needed, the date and time of the event and complete the submission, either including his/her identity or selecting to send a report where his/her personal data can be hidden (details on how this is implemented, on the privacy protection sub-section).

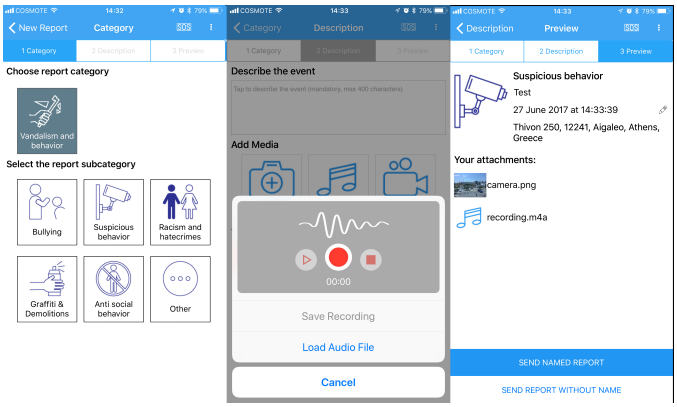

Figure 2: A new Report using the mobile phone application

Another basic feature is the preview of previously submitted reports; the user can preview them either on a table or as markers on a map, and get their details by selecting them. In a similar view (with the option to switch between a table and a map), the user can be informed about several events that are active on a nearby location to his/hers.

Except the web and mobile applications, the use of a wearable device such as a smart watch, is also offered. On a wearable device, a report can be created again in just three taps. A category is first chosen; a short message is either selected from a list of predefined messages or created using the watch's input capabilities (e.g. speech-to-text, scribble), and an audio recording of a few seconds can be made before the submission. The option to protect the user's identity is available here as well.

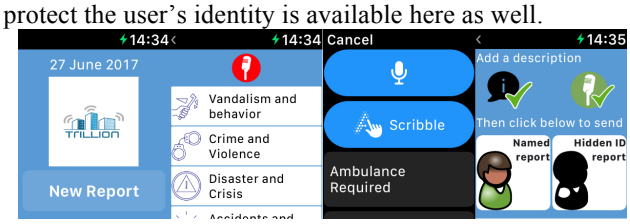

Figure 3: The smart watch version of the application

B. Reliability

The cyber trustworthiness monitoring system has been implemented as a service that runs in the background. It has been designed to be modular, bestowing the capability of being able to easily account for the different sensors, features and interfaces that are available on a mobile device without the need to redevelop the application. To enable this modularity, every monitoring module inherits from an abstract module superclass. The superclass contains attributes that are common among all modules, such as the time between samples to be collected and, provides concrete methods for controlling the function and logging of the modules. Also, a threaded generic module task is implemented in the superclass, which controls the behaviour of the modules. Moreover, this provides the advantage of each module being its own threaded process, allowing for different setting to be applied (e.g. sample rate) between modules. When a module has been started, it initially collects any constant variable data (e.g., what Wi-Fi security protocol is used, or whether the device has been jailbroken) and then collect data at set time intervals (e.g., network packets received since last time, or current number of satellites utilized for GPS localization). Modules can either collect samples indefinitely or a set number. The module sub-classes contain the actual implementations for collecting data from the sources of the device and, are required to implement the abstract methods of the superclass, which are invoked from the threaded generic module task. Lastly, a listener interface is also provided, which the modules publish on to alter listeners to changes in a module's state and response accordingly. For example, when a module has published finished, one may want to then process the data it has collected.

A reasoning component evaluates the likelihood of the device having been maliciously manipulated by testing against a machine learning model. A large variety of models have been

evaluated experimentally, most with high degree of accuracy. For the practical implementation, the chosen model is based on logistic regression, because evaluating it in real-time consumes very little resources, yet it still exhibits a high degree accuracy. In practice, the probability response provided by the model is what forms the automatic scoring (with 0% being a device that is certainly not trustworthy and 100% the device being completely trustworthy). This score is visualised to the user as a colour-coded icon on the top left of the device, where green means high trustworthiness, orange is medium and red is low).

C. Privacy Protection

In order to protect the user's privacy, a two-step communication gateway named "Privacy Protection Communication Gateway (PPCG)" has been implemented [20].

Two servers are included, with the first "Privacy Protection Proxy Server (PPPS)" having the responsibility to hide the identity of the reporting user, and the second "Control Centre Server (CCS)" to securely forward the report to the final destination. When a user selects to make a report without using his/her identity, an encrypted message is created, that contains a temporary AES key encrypted with the second server's public key, and the original report encrypted with aforementioned AES key. The user's private key (a key pair is generated on the first run of the application), is used to sign the message and his/her public key is also included on the message that is sent on the first server (PPPS). The later, after validating the signed data, removes the user's public key and replaces it with its own. After signing the new message (that no longer has any association with its original owner) with its own private key and sends the result to the second server (CCS). That server, after validating the signed from PPPS message, decrypts the AES key and then uses it to decrypt the received data. The decrypted data now are ready to be forwarded to their final destination. Any communication between the client, the two servers and the final endpoint is made through a secure channel using the Transport Layer Security (TLS) protocol.

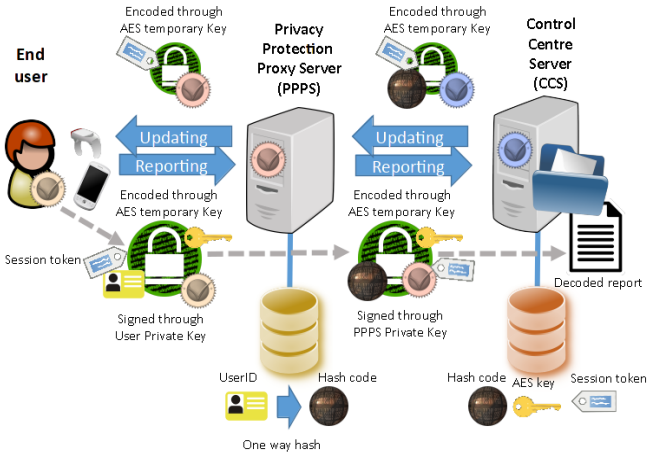

Figure 4: Privacy Protection Architecture

D. Training Using Serious Games

In order to train end users on the use of TRILLION platform, the use of serious games was adopted. The gaming application/platform (developed in TRILLION), and its mechanics, allow players to improve their awareness with respect to three growing levels (location, communication and interaction awareness).

Adopting the RAND approach presented earlier in the paper, the games' scenarios were designed having in mind the particular needs of technological and societal challenges. In this course:

- From the technological approach, scenarios are driven by how advances in technology are adopted and used by the intervenient actors.
- From the societal approach, scenarios are driven by how laws and law enforcement evolve and are viewed by the public, which will determine the effects of the evolution of society on law enforcement.

At the end of the game, citizens are encouraged to download the TRILLION apps (mobile and wearable) and use them in real life situations.

The architectural solution implemented for serious games is the client-server model. The client runs on desktop or mobile personal devices, being responsible for the computational part, while the server side provides data regarding the game list and data model linked to the selected game (items, characters, events, requirements, actions).

The main game elements are:

Items, which are objects scattered within the boundaries of the game area; they are not always useful to meet the challenge or solve the game itself (they could be used, by the game master, to divert the player's attention),

Characters, which are virtual people usually linked with an audio file,

Events, which represent something that is happening and that needs the intervention of the citizen, and

Actions, which are selected by the player once an event position is reached. In particular, the game proposes a list of actions to be dragged and dropped in the right order (one of the suggested action will encourage to report what is happening to the LEAs, using TRILLION app).

At the end of the game, a debriefing session provides the opportunity to learn different/better behaviors. The feedback session (debriefing) also aims to verify if the game reached the TRILLION SGs' goals:

- enable a collaborative gameplay;
- foster collaborative behavior;
- increase citizen awareness about collaboration with LEAs in urban security and risk management, which is the main objective of the citizen oriented gaming event.

IV. Conclusions

Community policing is gradually becoming synonymous to modern policing, but from a technological perspective, this

process is supported by disjointed initiatives, software tools and social media. The TRILLION project aims is producing a single platform, centered around a mobile app available to citizens, to support community policing in its different flavors. Towards an effective and efficient use of technology, supported by societal approval, the TRILLION app has been designed with an emphasis on usability of the app, trustworthy reports that have not been maliciously modified via cyber means, and protection of privacy that adapts to the privacy sensitivity of the citizen and local legislation. These three principles provide the basis for reliable use, and they are accompanied by a citizen awareness raised via a purpose-built serious game running on mobile devices. The overall platform is an ambitious offering, whose components are already evaluated in live trials in several locations in Europe, and in close collaboration with a variety of LEAs with remits that range from minor crimes to serious and organized crime, as well as emergency planning.

ACKNOWLEDGMENTS

This work is funded by the European Commission under grant number H2020-FCT-2014, REA grant agreement n° [653256]. The support is gratefully acknowledged.

REFERENCES

[1] Cordner, G., 2014. Community policing. The Oxford handbook of police and policing, pp.148-171.

[2] TRILLION: TRusted, CItizen - LEA coILaboratIon over sOcial Networks, http://trillion-project.eng.it, Deliverable 2.1 “Creation and Management of User Community“, 2017.

[3] Gill, C., Weisburd, D., Telep, C.W., Vitter, Z. and Bennett, T., 2014. Community-oriented policing to reduce crime, disorder and fear and increase satisfaction and legitimacy among citizens: a systematic review. Journal of Experimental Criminology, 10(4), p.399.

[4] Schanzer, D.H., Kurzman, C., Toliver, J. and Miller, E., 2016. The challenge and promise of using community policing strategies to prevent violent extremism: A call for community partnerships with law enforcement to enhance public safety. Triangle Center on Terrorism and Homeland Security.

[5] Dunn, K.M., Atie, R., Kennedy, M., Ali, J.A., O’Reilly, J. and Rogerson, L., 2016. Can you use community policing for counter terrorism? Evidence from NSW, Australia. Police Practice and Research, 17(3), pp.196-211.

[6] Lewis, S. and Lewis, D.A., 2012, May. Examining technology that supports community policing. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 1371-1380). ACM.

[7] Meijer, A.J. and Torenvlied, R., 2016. Social media and the new organization of government communications: An empirical analysis of Twitter usage by the Dutch police. The American Review of Public Administration, 46(2), pp.143-161.

[8] Anderson, M., Lewis, K. and Dedehayir, O., 2015, August. Diffusion of innovation in the public sector: Twitter adoption by municipal police departments in the US. In Management of Engineering and Technology (PICMET), 2015 Portland International Conference on (pp. 2453-2464).

[9] Sachdeva, N. and Kumaraguru, P., 2015, May. Social networks for police and residents in India: exploring online communication for crime prevention. In Proceedings of the 16th Annual International Conference on Digital Government Research (pp. 256-265). ACM.

[10] Park, S., Ilincai, E.S., Oh, J., Kwon, S., Mizouni, R. and Lee, U., 2017, May. Facilitating Pervasive Community Policing on the Road with Mobile Roadwatch. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (pp. 3538-3550). ACM.

[11] Welsh, D. and Roy, N., 2017, March. Smartphone-based mobile gunshot detection. In Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on (pp. 244-249).

[12] Siberglitt, R., Chow, B.G., Hollywood, J.S., Woods, D., Zaydman, M. and Jackson, B.A. (2015), Visions of Law Enforcement Technology in the Period 2024-2034, RAND Corporation, Santa Monica, Calif.

[13] C. Patrikakis, A. Konstantas, D. Kogias, M. Choras, “TRILLION project approach on scenarios definition for citizen security services”, to appear in International Journal of Electronic Governance, 2017.

[14] Carole Lucock, Valerie Steeves, Kerr, Ian , “Lessons from the identity trail : anonymity, privacy, and identity in a networked society”, Oxford University Press, 2009.

[15] S. Gritzalis, "Enhancing web privacy and anonymity in the digital era," Information Management & Computer Security, vol. 12, no. 3, pp. 255–287, 2004

[16] Crime Stoppers International, https://csiworld.org/, last accessed on July 2017.

[17] Rahman, S.S., Heartfield, R., Oliff, W., Loukas, G. and Filippoupolitis, A., 2017. Assessing the cyber-trustworthiness of human-as-a-sensor reports from mobile devices.

[18] Laurie, Graeme T. (2002): Genetic Privacy: A Challenge to Medico-Legal Norms (Cambridge University Press, Cambridge UK)

[19] Brey, P. (2007): Ethical Aspects of Information Security and Privacy, in: Security, Privacy, and Trust in Modern Data Management, M. Petković and W. Jonker (Eds.), Springer Berlin Heidelberg, pp. 21-36.

[20] C. Chatzigeorgiou, L. Toumanidis, D. Kogias, C. Patrikakis, E. Jacksch, “A Communication Gateway Architecture for Ensuring Privacy and Confidentiality in Incident Reporting”, in the 1st International Workshop on the Internet of People and Things (IPAT 2017), June 7-9, London, 2017.