European Commission
Directorate-General Home Affairs
Prevention of and Fight against Crime Programme

HOME/2010/ISEC/AG/INT/002

ForToo – Forensic Tools against Illegal Use of the Internet

D4: Dissemination Report

Work Package:	WP4: Dissemination
Contractual delivery date:	30 September 2014
Actual delivery date:	30 September 2014
Leading partner:	University of Bristol
Editor:	Theo Tryfonas (Project Coordinator, main author)
Contributors:	John May (quality reviewer)

With the support of the Prevention of and Fight against Crime Programme.
European Commission - Directorate-General Home Affairs

This project has been funded with the support of the *Prevention of and Fight against Crime* Programme of the European Commission - Directorate-General Home Affairs. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of Contents

TABLE OF CONTENTS **2**

1 SUMMARY **3**

2 PROJECT IDENTITY AND BRANDING **4**

2.1 CREATION AND USE OF LOGOS 4
2.2 PROJECT WEB SITE 4
2.3 T-SHIRTS 4

3 ACADEMIC PUBLICATION **5**

3.1 JOURNAL PUBLICATIONS (3) 5
3.2 CONFERENCE PAPERS (15) 5
3.3 POSTERS (3) 7

4 EVENTS **8**

4.1 INVITED TALKS AND KEYNOTES IN THIRD-PARTY EVENTS 8
4.1.1 UK Cybercrime Network kick off meeting 2012 ..... *8*
4.1.2 Invited lecture, Ionian University 2013 ..... *8*
4.1.3 Security and Protection of Information 2013 ..... *8*
4.1.4 HCI International 2013 ..... *8*
4.1.5 UK Cybercrime Network meeting 2014 ..... *9*
4.1.6 European Intensive Programme on Information and Communication Security 2014 ..... *9*
4.2 DEDICATED FORTOO EVENTS 9
4.2.1 WDFIA/IFIP SEC 2012, Crete *9*
4.2.2 Close-out workshop 2014, Brussels *10*

5 IMPLEMENTATION GUIDE AND TUTORIALS **11**

5.1.1 D3/DFRWS EU submitted paper *11*
5.1.2 UoB InfoSoc tutorials *11*

6 SIGNIFICANCE, EARLY IMPACT INDICATIONS AND LEGACY **12**

6.1 QUALITY OF SCIENCE 12
6.2 LINKS TO OTHER EUROPEAN INITIATIVES 12
6.2.1 NIFTy project *12*
6.2.2 FRUITS bid *12*
6.2.3 eWatch bid *13*

1 Summary

This report summarises the dissemination activities of the project **ForToo**, the outreach results achieved so far, and discusses plans to manage the legacy of the project upon its closure. The activities documented include full details of academic publication in relevant journals, conferences and posters, outreach activities such as seminars, invited talks and keynotes in third party events, and finally dedicated events organised either as part of our scheduled dissemination plan, or as ad hoc instances where opportunity arose.

2 Project identity and branding

2.1 Creation and use of logos

FORTH was responsible for developing the visual identity of ForToo and early in the project developed candidate logos of which the partners all agreed to use the one appearing on the site, posters and the covers of all deliverables. It can be seen in FIG 1. The partners felt that the logo combines nicely the project's acronym with an image suggestive of digital technology examination, through the circuitry and the magnifier depicted.

Figure 1: Core project logo.

2.2 Project web site

The project's web site is hosted at the URL http://www.fortoo.eu/. It is maintained regularly by FORTH and it contains public pages with information on the project, profiles of participating partners and a list of academic publications disseminating project outcomes. Other content that can be found on-line include references and photographs from out events, including video of our 2012 workshop held as part of IFIP/SEC of that year.

The site also includes a private section. The private section of the project's page provides access to a protected on-line repository, which hosts deliverables, documents and source code. This can be accessed and managed remotely through a software and content versioning system, the Apache Subversion (SVN).

2.3 T-shirts

As part of our dissemination strategy we also printed T-shirt with the project's logo. This were handed out to participants of our close out workshop and to other selected individuals that had relationships with the research or had participated in project events. The T-shirts can be seen packaged in FIG 2.

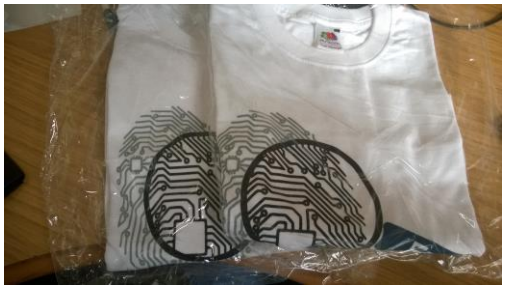

Figure 2: T-shirts featuring the project logo.

3 Academic publication

Overall, all output below represents work conducted within the scope of the project's various workpackages and is collaboration between consortium members, but also on occasion with external third parties.

3.1 Journal publications (3)

[1] Vijay Kumar, George Oikonomou, Theo Tryfonas, Dan Page, Iain Phillips. Digital investigations for IPv6-based Wireless Sensor Networks. *Digital Investigation, Elsevier, 11, Supplement 2(0), pp. S66-S75, 2014 (Fourteenth Annual DFRWS Conference). August* 2014.

[2] Panagiotis Andriotis, George Oikonomou, Theo Tryfonas, "JPEG Steganography Detection with Benford's Law", Digital Investigation, Elsevier, vol. 9, no. 3-4, pp. 246-257, 2013.

[3] Panagiotis Andriotis, Zacharias Tzermias, Anthi Mparmpaki, Sotiris Ioannidis, George Oikonomou, Multilevel Visualization Using Enhanced Social Network Analysis with Smartphone Data. *International Journal of Digital Crime and Forensics*, IGI Global, 2013.

3.2 Conference papers (15)

All papers listed below have been presented at the respective events by one or more members of their authoring team. Every effort was made for a ForToo member to present the paper where possible, given the fact that some of the papers represent collaborations with external colleagues from academia and industry. Travel has been predominantly funded by the consortium as part of the co-financing expenditure, unless otherwise stated besides each citation. Trips funded directly by the grant will appear individually in the final financial reporting.

[4] Alexandros Fragkiadakis, Pavlos Charalampidis, Stefanos Papadakis, Elias Trago. Experiences with deploying Compressive Sensing and Matrix Completion techniques in IoT devices. IEEE 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD). December 2014, Athens, Greece. (to appear)

[5] Despoina Antonakaki, Iasonas Polakis, Elias Athanasopoulos,Sotiris Ioannidis, Paraskevi Fragopoulou. Think before RT: An Experimental Study of Abusing Twitter Trends. Workshop on Social Influence (SI), November 2014.

[6] Iasonas Polakis, Panagiotis Ilia, Federico Maggi, Marco Lancini, Georgios Kontaxis, Stefano Zanero, Sotiris Ioannidis, Angelos D. Keromytis. Faces in the Distorting Mirror: Revisiting Photo-based Social Authentication. In proceedings of the 21st ACM Conference on Computer and Communications Security (CCS). November 2014, Arizona, USA.

[7] Martina Lindorfer, Stamatis Volanis, Alessandro Sisto, Matthias Neugschwandtner, Elias Athanasopoulos, Federico Maggi, Christian Platzer, Stefano Zanero, Sotiris Ioannidis. AndRadar: Fast Discovery of Android

Applications in Alternative Markets. In proceedings of the 11th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA). July 2014. London, UK.

[8] Panagiotis Andriotis, Theo Tryfonas, George Oikonomou. Complexity metrics and user strength perceptions of the pattern-lock graphical authentication method. In proceedings of the 16th International Conference on Human-Computer Interaction (HCI 2014). June 2014. Heraklion, Crete, Greece.

[9] Zacharias Tzermias, Vassilis Prevelakis, and Sotiris Ioannidis. Privacy Risks from Public Data Sources. In Proceedings of the 29th IFIP International Information Security and Privacy Conference (SEC). June 2014, Marrakech, Morocco.

[10] Panagiotis Andriotis, Atsuhiro Takasu and Theo Tryfonas. Smartphone Message Sentiment Analysis. Advances in Digital Forensics X, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, 2014.

[11] Antonis Papadogiannakis, Laertis Loutsis, Vassilis Papaefstathiou and Sotiris Ioannidis ASIST: Architectural Support for Instruction Set Randomization. In proceedings of the 20th ACM Conference on Computer and Communications Security (CCS). November 2013, Berlin, Germany.

[12] Dana Polatin-Reuben, Richard Craig, Theodoros Spyridopoulos and Theo Tryfonas. A System Dynamics Model of Cyber Conflict. In proceedings of the 2013 IEEE International Conference on Systems, Man, and Cybernetics (IEEE SMC2013). October 2013, Manchester, England.

[13] Panagiotis Andriotis, Theo Tryfonas, George Oikonomou, Theo Spyridopoulos, Alex Zaharis, Adamantini Martini and Ioannis Askoxylakis, On Two Different Methods for Steganography Detection in JPEG Images with Benford's Law, In proceedings of the 7th Scientific NATO Conference in Security and Protection of Information (SPI 2013). May 2013, Brno, Czech Republic.

[14] Evangelos Ladakis, Lazaros Koromilas, Giorgos Vasiliadis, Michalis Polychronakis and Sotiris Ioannidis You Can Type, but You Can't Hide: A Stealthy GPU-based Keylogger, In proceedings of the 6th European Workshop on Systems Security (EuroSec), April 2013, Prague, Czech Republic.

[15] Panagiotis Andriotis, Theo Tryfonas, George Oikonomou and Can Yildiz, A Pilot Study on the Security of Pattern Screen-Lock Methods and Soft Side Channel Attacks, In proceedings of the 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec). April 2013, Budapest, Hungary

[16] Panagiotis Andriotis, George Oikonomou and Theo Tryfonas, Forensic Analysis of Wireless Networking Evidence of Android Smartphones, In proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS). December 2012, Tenerife, Spain.

[17] Eleni Gessiou, Stamatis Volanis, Elias Athanasopoulos, Evangelos P. Markatos, and Sotiris Ioannidis. Digging up Social Structures from Documents on the Web. In proceedings of the IEEE Global Communications Conference (GLOBECOM). December 2012, Anaheim, CA, USA.

[18] Iasonas Polakis, Marco Lancini, Georgios Kontaxis, Federico Maggi, Sotiris Ioannidis, Angelos Keromytis, and Stefano Zanero. All Your Faces Are Belong to Us: Breaking Facebook's Social Authentication. In proceedings of the Annual

Computer Security Applications Conference (ACSAC). December 2012, Orlando, FL, USA.

3.3 Posters (3)

[19]Panagiotis Andriotis, Theo Tryfonas and Zhaoqian Yu. **Breaking the Android Pattern Lock Screen with Neural Networks and Smudge Attacks**. *7th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*. July 2014, Oxford, UK.

[20] Panagiotis Andriotis, Theo Tryfonas, George Oikonomou, Shancang Li, Zacharias Tzermias, Konstantinos Xynos, Huw Read and Vassilis Prevelakis. **On the Development of Automated Forensic Analysis Methods for Mobile Devices.** *7th International Conference on Trust & Trustworthy Computing (TRUST)*. July 2014, Heraklion, Crete, Greece.

[21]Panagiotis Andriotis, George Oikonomou, Theo Tryfonas. **Forensic Analysis of Wireless Networking Evidence of Android Smartphones.** *Information Assurance Advisory Council Annual Symposium*. September 2012, London, UK.

4 Events

4.1 Invited talks and keynotes in third-party events

The list of events below excludes regular conference presentations where ForToo researchers attended and presented their work as part of regular proceedings. The events include invited sessions and other targeted dissemination actions.

4.1.1 UK Cybercrime Network kick off meeting 2012

The Cybercrime Network is a UK national forum funded by EPSRC and coordinated by Newcastle University, which brings together law enforcement personnel with practitioners and academics from the field of digital forensics. The meetings are usually focussed on a current forensics challenge and participants debate aspects of the future as well as presenting their current relevant work. In its kick off meeting on 11 November 2012, Theo Tryfonas (UNIVBRIS) presented an outline of the project and its objectives along with some preliminary results.

4.1.2 Invited lecture, Ionian University 2013

Theo Tryfonas (UNIVBRIS) was invited as the project's Coordinator to deliver a mini-series of lectures related to steganography detection and mobile authentication to Ionian University in Corfu, Greece. The lectures took place as a half-day session on these topics and all materials were made available to the attendees in the form of lecture note hand outs. The session was organised on 15 May 2013.

4.1.3 Security and Protection of Information 2013

Theo Tryfonas (UNIVBRIS) delivered an invited talk at the 7th International Scientific NATO-sponsored conference on Security and Protection of Information (SPI 2013), an event that is held bi-annually in Brno, Czech Rep. That year the conference ran from 22-24 May.

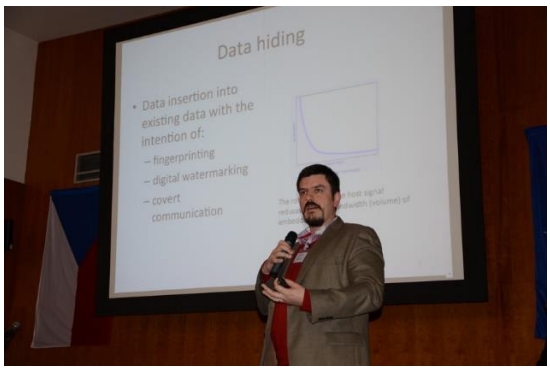

Figure 3: T. Tryfonas addressing a full room on the opening day of SPI 2013 at Brno, Czech Republic.

The talk addressed issues of steganography detection in JPEG images from a forensic perspective and presented the outcomes of our work as documented in our relevant publication in Digital Investigation ([2] from the list of section 3.1). The audience comprised predominantly NATO armed forces and local law enforcement personnel, besides academics and practitioners working in the fields of cybersecurity and digital forensics.

4.1.4 HCI International 2013

Theo Tryfonas (UNIVBRIS) delivered insights into the project's outcomes as part of a tutorial organised in the context of HCI International 2013. This is a large scale conference (over 2,000 delegates) and a key event of the scientific field of human-

computer interaction. The 2013 event was organised in Las Vegas, Nevada U.S., and took place from 21-26 July. This half-day tutorial was delivered on 23rd July.

Theo presented the ForToo work relating to the pattern lock authentication attacks, as part of a state of art tutorial in the area of mobile authentication security. This work has been documented predominantly in the academic publication [15] listed in section 3.2.

4.1.5 UK Cybercrime Network meeting 2014

George Oikonomou (UNIVBRIS) presented work on IoT forensics conducted as part of ForToo's emerging networks forensics activity. The meeting took place on 17th July 2014. The talk was based on materials presented subsequently to DFRWS 2014 and was published as a paper in a special issue of Digital Investigation (publication [1] from 3.1).

4.1.6 European Intensive Programme on Information and Communication Security 2014

Panagiotis Andriotis (UNIVBRIS) delivered an invited session during the 17th European Intensive Programme on Information and Communication Security (IPICS), an annual European summer school targeted at early doctorate candidates and postgraduate researchers. That year it took place in Mytilene, Greece in July 2014. Panagiotis presented the JPEG steganography detection methods, the pattern lock attacks and also spoke about the examination of digital evidence from social networking activity and its challenges.

4.2 Dedicated ForToo events

4.2.1 WDFIA/IFIP SEC 2012, Crete

On 8th June 2012 we organised an expert panel during the Workshop in Digital Forensics and Incident Analysis that took place alongside IFIP's annual Information Security and Privacy Conference in Crete, Greece (IFIP SEC 2012). Under facilitation from Sotiris Ioannidis (FORTH), ForToo's Technical Coordinator, a panel of invited experts debated the current challenges and areas of emerging interest in the field of digital forensics. Key points of this workshop were taken on board by the project consortium to facilitate and guide further work, both within the scope of ForToo and also of affiliated projects.

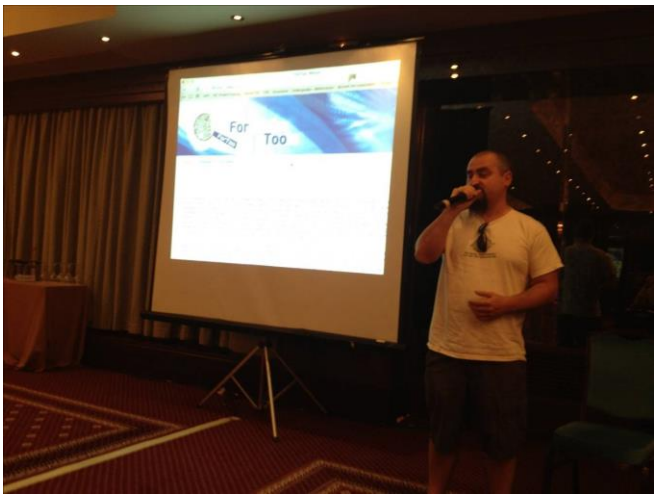

Figure 4: S. Ioannidis facilitates the panel discussion at Creta Maris Hotel during IFIP/SEC 2012 in Crete, Greece.

As an example of the latter, the work on digital camera identification that was suggested as a key challenge was subsequently taken further through the HOME DG funded project NIFTy, which was funded under the ISEC 2012 Action

Grants (ref. HOME/2012/ISEC/INT/4000003892). Some of the other concerns discussed (e.g. privacy preserving investigations and on-line safety, are further addressed through our recent bids FRUITS and eWatch). Details of these initiatives will be presented subsequently.

The panellists included:

- Dr. Konstantinos Moulinos (ENISA resilience expert and Hellenic Data Protection Authority auditor);
- Dr. Nathan Clarke (University of Plymouth academic);
- Professor Chang-Tsun Li (Warwick University academic); and
- Ms. Meltini Christodoulaki (SafeLine GR legal expert).

A video of the panel discussion can be found for viewing and downloading under the 'Events' section of ForToo's website. It was kindly recorded by members of staff from Plymouth University who were co-organising the WDFIA host event.

4.2.2 Close-out workshop 2014, Brussels

With the kind permission of the Commission, we decided to reconfigure part of our remaining budget in order to organise and deliver a final dissemination event in order to promote the project's outcomes and also to solidify its legacy. At a relatively short notice the event was not intended to attract large number of attendees, but instead to:

- Inform a representative range of selected key stakeholders about the activities taken and the outputs produced through the course of the project;
- Solicit feedback on the outputs from key representative stakeholders of forensics practice, both from private industry and law enforcement;
- Publicise the legacy of the project to attract stakeholder interest and engage them early into the ideas of current or forthcoming bids; and
- Develop further relationships with those stakeholders.

The workshop took take place on 30 September 2014 and besides the consortium partners, the delegates included indicatively:

- academics and researchers from Newcastle (UK), Noroff UC (NO) and KU Leuven (BE) universities;
- senior managers from HP Enterprise Security Services (UK), BAE Systems Applied Intelligence (UK) and Aconite Internet Solutions (IE).
- EC staff members, including the ForToo Project Officer and CERT-EU personnel.

Open invitations had also been circulated to a number of other stakeholders including academics, law enforcement and officers from ENISA, DG CONNECT, Trust & Security and EU Cert. A full, signed participants list has been kept and will be provided with the documentation of the final reporting.

Summary notes from the workshop will be drafted and disseminated later to all participants as a reference and aid memoir when in preparation of potential bids for forthcoming Horizon or other related funding.

5 Implementation guide and tutorials

5.1.1 D3/DFRWS EU submitted paper

As a way of assisting potential third party forensic tool developer in integrating their own applications with the DEViSE platform we have published D3 that contains the integration specification, a user guide for the platform and a case study illustrating integration of ForToo tools with respect to examination of social networking evidence that come from mobile phones. The latter comes in the form of a draft paper submitted for publication with the Digital Forensics Research Workshop EU 2015; the outcomes of the peer-review process are not known at the time.

5.1.2 UoB InfoSoc tutorials

As part of a student-led series of seminars in information security at the University of Bristol, we organised two hands on tutorials on forensic tools. This was in order to showcase and provide training on our open toolset to students, but also to the community, as the events were open for everyone to attend and publicised widely, especially among local practice communities through relevant University mailing lists.

The programme consisted of the following tutorials

- **Introduction and open source toolkits for computer forensics** (Wednesday 11 Dec 2013, 4-6pm): a discussion on what is computer forensics, basic principles, some generic references to existing tools (e.g. using the dd command for evidence acquisition, evidential integrity verification with the md5/SHA-2 hashing algorithm etc.); and
- **Specialised topics in computer forensics** (Wednesday 18 Dec 2013, 4-6pm): a hands on session on mobile phone evidence acquisition from Android and steganography detection in JPEG images using the ForToo methods and toolkit.

Presentation slide handouts and copies of the tools used where provided to all participants.

6 Significance, early impact indications and legacy

6.1 Quality of science

Over the three years and three months of the project's eventual duration the consortium achieved the publication of 3 journal papers, 15 conference papers and 3 posters, with other two submissions sponsored by this grant pending for peer-review at the time of writing this deliverable. This is an average of about 7 publications per year and it includes effort between the consortium partners, but also joint research with external collaborators demonstrating the wider reach of ForToo's research base.

Among the venues of publication were include top security (e.g. ACM CCS, ACSAC, ACM WiSec, IFIP SEC) and forensics (IEEE WIFS, DFRWS, IFIP DF) conferences (e.g. papers [6,9,15,18] and [1,10,16]). All the aforementioned venues have typical acceptance rates below 30%. This demonstrates the penetration of the key outcomes of the project and the interest from the community in them. Few of the papers have already received a significant number of citations, even though they have been only published very recently. Papers [15] and [16] from section 3.2 have achieved double digit-citation figures within a year of publication (as computed by Google Scholar at the time of writing).

6.2 Links to other European initiatives

6.2.1 NIFTy project

Exploratory initiatives that took place during the course of the project led to alignment with subsequent research, also funded by DG HOME under ISEC. In particular, the work on digital camera identification that was suggested as a key challenge in our 2012 workshop was subsequently taken further through the HOME DG funded project NIFTy, which was funded under the ISEC 2012 Action Grants (ref. HOME/2012/ISEC/INT/4000003892). This represents an excellent form of capitalising on expertise and outcomes built on earlier rounds of ISEC funding by contributing towards further research; our role in this grant was to work on the analysis of contextual digital evidence, e.g. examination of EXIF data or file system attributes that may cross validate a line of inquiry.

Some of the other concerns explored (e.g. privacy preserving investigations and on-line safety), were further addressed through our recent bids FRUITS and eWatch respectively (both submitted August 2014), abstracts and consortia of which are given subsequently.

6.2.2 FRUITS bid

Abstract: The project aims to devise novel privacy-preserving forensic readiness techniques for smartphone applications and cloud services. Through these, end users will be able to protect the privacy of their personal data at the point of collection and transmission (on their smartphone) as well as at the point of storage (in the cloud). They will be able to audit the service provider in order to verify the correct handling of their personal data and identify cases of potential misuse. Thus, end users will have

better control of their data in terms of (i) what is being collected; (ii) where they are stored; (iii) how long they are stored for; (iv) for what purpose / how they are being used; and (v) the data's financial value to the user and to the service provider. At the same time, it is important to ensure that advanced privacy-enhancing techniques are not being misused to hide malicious or illegal activities. Therefore the techniques and tools devised by this project will be enhanced by forensicreadiness mechanisms, in order to facilitate digital investigation by law enforcement agencies.

The FRUITS consortium is carefully selected to bring together expertise in security and privacy in general, but more specifically, experts from complementary scientific excellence relevant to the project, including Internet of Things (in this case, smartphone and cloud), quantification, and digital forensic from academia, as well as software developers and service providers from industry. Coupled with the presence of key end users (software development house and law enforcement agency) in the consortium, the project is well placed to achieve its ambitious yet practical vision, which can make positive impact to the privacy of individuals while facilitating careful handling of sensitive data in forensic investigation.

Partners: Newcastle Univ. (UK), Univ. of Bristol (UK), Metropolitan Police (UK), FORTH (GR), Noroff Univ. College (NO), Darmstadt University (DE), Cyta Hellas (GR), and others.

6.2.3 eWatch bid

Abstract: Over the past few years we have been witnessing an alarming increase of the fear of crime, all over Europe, and especially in the countries of the European South. Fuelled by the ever-deepening crisis, ordinary crime has spread in our neighbourhoods and the fear of crime has taken deep roots in our hearts. This prevalent feeling of fear leads more and more people to withdraw into the perceived safety of their homes, into the reduced circle of their immediate family, and eventually into the loneliness of their isolation.

In this project we advocate a game-changing approach to break the feeling of isolation and shatter the fear of crime by capitalizing on two powerful forces which have revolutionized their fields: community policing and on-line social networks. We advocate the use of dynamically-created bottom-up on-line social networks as the major means to increase citizen interaction so as to give people back their long-lost feeling of community. At the same time, we lower the barriers of communication between police and citizens by making use of agile digital reporting mechanisms. Packaging both interaction and reporting into a novel push-based approach for smartphone environments, we empower ordinary citizens and we make community policing an effortless and effective part of their normal daily routine.

Partners: FORTH (GR), Univ. of Bristol (UK), Edinburgh Napier Univ. (UK), Metropolitan Police (UK), Aconite Internet Solutions (IE), Institut Jozef Stephan (SI), Smile of Child (GR), Nicosia Municipal Police (CY), and others.