Intelligent Information System Supporting
Observation, Searching and Detection for
Security of Citizens in Urban Environment

European Seventh Framework Programme
FP7-218086-Collaborative Project

D0.6 INDECT – Ethical Issues – 2010

The INDECT Consortium

AGH – University of Science and Technology, AGH, Poland
Gdansk University of Technology, GUT, Poland
InnoTec DATA GmbH & Co. KG, INNOTEC, Germany
Grenoble INP (Ensimag), INP, France
MSWiA1 - General Headquarters of Police (Polish Police), GHP, Poland
Moviquity, MOVIQUITY, Spain
PSI Transcom GmbH, PSI, Germany
Police Service of Northern Ireland, PSNI, United Kingdom
Poznan University of Technology, PUT, Poland
Universidad Carlos III de Madrid, UC3M, Spain
Technical University of Sofia, TU-SOFIA, Bulgaria
University of Wuppertal, BUW, Germany
University of York, UoY, Great Britain
Technical University of Ostrava, VSB, Czech Republic
Technical University of Kosice, TUKE, Slovakia
X-Art Pro Division G.m.b.H., X-art, Austria
Fachhochschule Technikum Wien, FHTW, Austria

© Copyright 2010, the Members of the INDECT Consortium

[1]MSWiA (Ministerstwo Spraw Wewnętrznych i Administracji) – Ministry of Interior Affairs and Administration. Polish Police is dependent on the Ministry

Document Information

Contract Number	*218086*
Deliverable name	*INDECT – Ethical Issues – 2010*
Deliverable number	*D0.6*
Editor(s)	*Jan Derkacz, AGH -UST* *derkacz@kt.agh.edu.pl* *Mikołaj Leszczuk, AGH-UST* *leszczuk@agh.edu.pl*
Author(s)	*Jan Derkacz,* *Drew Harris, Mikołaj Leszczuk,* *Emil Pływaczewski,* *Andreas Pongratz, Ralph Roche,* *Zulema Rosborough,* *Tom Sorell* *Mariusz Ziolko*
Reviewer(s)	*Professor Andrzej Dziech*
Dissemination level	*Public*
Contractual date of delivery	*31/03/2011*
Delivery date	*31/03/2011*
Status	*Final Version*
Keywords	*Ethics Board, ethical issues*

This project is funded under 7th Framework Program

Table of Contents

(This page is left blank intentionally)

1 Executive Summary

The document has for objective to give an overview of activities relevant to ethical issues within INDECT during the second year of project work.

In the first part, the document shows a summary of actions undertaken: Ethics Board meetings, contacts with other projects and events at which INDECT was present. Deliverables which have been reviewed from the ethical point of view are listed.

Section 4 presents exploitation of results and ethical challenges encountered by different INDECT Work Packages.

Section 5 contains INDECT Synopsis clarifying the actual INDECT Project research, objectives and expected outcomes.

The main conclusions concerning ethical issues are the final part of the deliverable.

2 Introduction

Security of citizens is one of the most important priorities of EU. This fact has been emphasized in the Fourth European Security Research Conference in Stockholm, 29th-30th September, 2009. For EU FP7 Research Programme, Security call has been announced in 2007.

INDECT project has been initiated by the Polish Platform for Homeland Security (http://www.ppbw.pl/en/index.html). The Project proposal was submitted by the international, pan-European consortium of 17 partners, led by the AGH University of Science and Technology (Krakow, Poland), under the supervision of Professor Andrzej Dziech, the INDECT Project Coordinator. The consortium consists of 11 well-known universities, 4 companies and 2 end-users (Police Service of Northern Ireland and Polish General Headquarters of Police). **It should be underlined that the INDECT project is a research project**, allowing involved European scientists to develop new, advanced and innovative algorithms and methods aiming at combating terrorism and other serious criminal activities, such as organised crime, affecting citizens' safety.

The INDECT project is a standard Seventh Framework Programme (FP7) research project. The project is financed under the Security Theme of FP7. The legal basis of the Security Theme is Council Decision 2006/971/EC[2]. The INDECT project started on the first of January 2009 for duration of 60 months.

[2] 2006/971/EC: Council Decision of 19 December 2006 concerning the Specific Programme Cooperation implementing the seventh framework programme of the European Community for research, technological development and demonstration activities (2007-13), OJ L 400, 30.12.2006.

3 Actions undertaken during the second year of the project

This document section shows a summary of actions undertaken: Ethics Board meetings, contacts with other projects and events at which INDECT was present. Deliverables which have been reviewed from the ethical point of view are enumerated.

3.1 Ethics Board meetings

INDECT Ethics Board meeting, Florence 18-19 February 2010

Ethics Board meeting in Florence was collocated with DETECTER meeting where INDECT project was presented. Information relevant to the meeting is given in section 3.2.

INDECT Ethics Board Video Conference, 22 October 2010

Introduction and Welcome

Mr Harris opened the video conference by welcoming everyone and expressed his gratitude to all members present for their attendance.

Attendees:

Name	Organisation
Mr Harris	PSNI
Zulema Rosborough	PSNI
Andreas Pongratz	X-Art, Austria
Plamen Vichev	TUS, Bulgaria
Gerry Murray	PSNI
Michael Ross	PSNI
Jan Derkacz	AGH, Poland
Tom Sorell	Birmingham University
Ralph Roche	PSNI
Piotr Szczuko	WP1
Suresh Manandhar	WP4
Mikolaj Leszczuk	WP5
Manuel Urueña	WP8

3.0 Apologies

Name	Organisation
Helen Petrie	University of York
Mariusz Ziolko	AGH University, Poland
Gema Maestro	WP6
Patrick Hasenfuss	WP7

Minutes of last Meeting

Agreed.

Presentations from Work Package Leaders
There followed a series of presentation on behalf of each work package.

Questions arising from Presentations:

- WP 1 Presented by Piotr Szczuko
- WP 2 Presentation attached
- WP 4 Presented by Suresh Manandhar
- WP 5 Presented by Mikolaj Leszczuk
- WP 6 Presentation attached
- WP 7 Presentation attached
- WP 8 Presented by Manuel Urueña

Questions arising from Presentations

The presentation was followed by a question and answer session.

In conclusion Mr Harris proposed that in relation to any on-going issues the next scheduled face to face meeting would provide an opportunity for continued discussion.

Review of Deliverables

Mr Harris thanked all Work Package Leaders for their presentations and reminded members that the Ethics Board requires a summary of deliverables prior to submission for review by the members of the Board. While some work package leaders are achieving this others are not. Mr Harris requested that all Work Package Leaders co-operate.

This requirement emanated from the Ethics Board meeting in Belfast when it was decided that two members of the Ethics Board would be responsible for the review of each Work package. It is acknowledged that as there is a tight time frame for the review process and as the deliverables are sizeable documents, and with the Board members not having the technological expertise, the provision of a summary would enable reviews to be completed in a more efficient and timely manner.

Action: Create an agenda item for next meeting – on Resources

Correspondence/Media Attention

Discussion took place surrounding a proposal in the European Parliament which is likely to be adopted, focusing on transparency. It was agreed that while certain aspects of research should

remain confidential the Ethics Board would propose that as much as possible remain in the public domain.

Within Europe there has also been quite intense press and political interest in INDECT funding and while some of the criticism has to be accepted aspects remain unjustified in light of the evidence.

In support of on-going openness Mr Harris has agreed that his photograph should be included on the public website. As for all remaining members of the Board this decision would be their own personal choice.

Any other Business

Plamen Vichev tendered his resignation from the INDECT Ethical Board. Mr Harris thanked Plamen for his contribution and support and that while accepting the resignation requested that he formalise this in writing to the Chair. This Plamen agreed to undertake.

It was discussed that perhaps Skype could be used for future remote conferences.

Mr Harris proposed that the Ethics Board should undertake more face to face meetings in order to manage through Ethical issues associated with the project.

Action: Sadhbh McCartney to be invited to attend next Ethics Board meeting

Date of next meeting

Date of next meeting was agreed for 31st January 2011 and 1st February 2011 in Belfast. All Work Package Leaders are to be invited to attend also.

3.2 External contacts

DETECTER project conference – Florence 18th – 19th February 2010

An invitation had been extended to the INDECT project to deliver a presentation during the meeting of the DETECTER project which took place on 19th February 2010 in Florence.
It was decided to collocate INDECT Ethics Board meeting with the event.

INDECT Ethics Board was represented at DETECTER meeting where an overview of INDECT work and expected results were presented. The presentation was followed by a vivid discussion on ethical issues concerning tools elaborated within INDECT.

INDECT in Florence was accused in the Q&A of an overly wide application to problems of serious crime, terrorism and child pornography – it was accused of exaggerating the usefulness in tackling such problems – the use for terrorism attacked as a marketing gimmick.
Some had problems with searching for images as too blunt a tool – a number in the consortium didn't like the idea of it being used to find that someone had an image of a swastika in a file. Re. child pornography it was pointed out that some images can be manufactured without involvement of any child.
Consortium members claimed that it made much pointless surveillance more likely just by

virtue of making it much easier, that there was a big problem for this project re. 'chill', and that much of the technology had risks of discrimination.

Re. abnormal detection with e.g. smart cameras, we asked follow up questions about training provided for operators.

DETECTER project conference – Zurich - 10th -11th June 2010

The main subject of the conference was "Data Mining and Human Rights in the Fight against Terrorism". INDECT representatives presented tools for analysis of data content. After the presentation a number of questions concerning ethical and privacy issues were answered. Most of them were a subject to multilateral discussion.

Xplico

In the Zurich Q&A similar concerns were noted as were raised for INDECT about what kinds of files are treated as 'illegal' and warranting detection – we asked a follow up about building in restrictions for what kind of images etc. could be searched for.

In Q&A "deep concern was expressed by consortium members as well as the intelligence representative that there seemed to be nothing preventing undesirable access to this technology (one cited the example of the Siemens Iran case)".

Consortium members didn't like the fact that it was open source (which they seemed to think was a merit).

European Joint Conference of the HOPE and RISE projects

INDECT representative took part in The European Joint Conference of the HIDE and RISE Projects entitled "Ethics and Governance of Biometrics and Identification Technologies" which took place Brussels, 9th and 10th December 2010.

The conference had for the main objective to promote involvement of regulators, responsible agencies, law-making bodies, industry, third party privacy solutions providers and consumer representatives in setting technology security policy in Europe.

3.3 Deliverables reviewed

9.7 Intelligent portal for crisis management - functional specification and conceptual architecture
9.8 MANET physical layer analysis, MANET MAC layer analysis, MANET routing protocol analysis, MANET self-positioning algorithms analysis
7.2 Creation of different model of event in order to detect dangerous events
2.2 Description of systems architecture
2.3 Report on proposed algorithms for positioning tracking and predicting of the position of tracked objects
2.4 Report on the proposed algorithms and mechanisms for wireless transfer of partitioned spatial data
2.5 Report on the proposed algorithms and methods for autonomous steering and navigation of UVAs
2.6 Report on the proposed algorithms and mechanisms for cooperation within groups of autonomous UVAs
2.7 Report on the proposed algorithms for mission planning for groups of autonomous UVAs

3.2 Description of INDECT-MAS architecture
3.3 Report on content and behavioural pattern analysis techniques and tools
4.3 Report on current state-of-the-art on machine learning methods for behavioural profiling
4.4 System for enhanced search: tool for pattern based information retrieval
5.1 Preliminary report on police and prosecutor repositories and access procedures
8.2 Evaluation of components
9.10 Data formats and protocols for information handling in INDECT portal
9.11 Ontology and automatic reasoning in crisis management - definitions and concepts
9.47 Report on the outcomes of the first conference related to security of citizens in urban environment
1.2 Report on NS and CS hardware construction
6.2 Intelligent portal for crisis management - functional specification and conceptual architecture
7.3 Biometric features analysis component based on video and image information
4.5 Novel algorithms for relationship mining including comparison with existing methods indicated in 4.2
8.3 Specification of new constructed block cipher and evaluation of its vulnerability to errors
9.12 QoS for MANET analysis, security in MANET analysis
9.13 New block ciphers

4 Exploitation of results and compliance of INDECT work with Ethical Rules

In the INDECT Project, all exploitation activities are coordinated and managed by the project coordinator. Target users are precisely defined and analysed in terms of specific needs and objectives, through the involvement of all partners in the common discussion and specification of target population, contents and objectives.

This chapter gives an overview of different project Work-Packages (WP1 – WP8) with respect to ethical issues relevant to tools and methods elaborated in specific research and development areas. Potential challenges are presented together with measures that can be taken in order to prevent possible threats against privacy and civil rights.

4.1 Work-Package 1 – Intelligent Monitoring and Automatic Detection of Threats

The goal of this Work-Package is acquisition and analysis of audio and video streams from large number of cameras and microphones. The objective is automatic, intelligent detection of threats for safety: dangerous events and sounds. Sound events detection and classification is planned. Examples include gunshot, explosion, scream, crying for help in European languages, breaking glass. Detection of such events would enable identification of potential threats in real time and to undertake, without delay, all necessary steps proportionally to a specific threat (for example, burglary or robbery on banks that are difficult to identify visually in the night). Furthermore, techniques for sound source localization will be demonstrated. This means pointing moving PTZ (Pan-Tilt-Zoom) cameras at the source and streaming both audio and video from the event. Methods for content access protection with digital watermarking (for protecting Personally Identifiable Information – PII) will be applied. High quality of CCTV streams will be ensured using Quality of Experience methods.

Sensitive data in video content are anonymized by automatic obscuration of faces and car plate numbers, and by sending original information in encrypted form. Similarly, for the sound stream, only the processing results are presented and sensitive recordings are encrypted. Therefore the operator has a possibility to review the event without violating privacy rights, and only after specific access rights were issued he can replay the original material.

4.2 Work-Package 2 – Identification and Observation of Mobile Objects in Urban Environment

Work-Package 2 (WP2) – will provide tools for identification and observation of mobile objects in urban environment. The objective of WP2 is to support operational activities of police officers and other public services with a techniques and tools for the observation of various mobile objects. This will be done with the use of integrated network-centric system consisting of: INDECT UAV, Automatic Plate Recognition Station, Blue-Force Tracking Devices and Small Tracking Devices. The INDECT UAV will be featured by exchangeable gimbal with daylight or thermal 10x zoom camera, ability of lifting off from a trolley or catapult, easy dismount-ability (longest part has 80 cm), easily exchangeable batteries as well as light weight (6 kg).

Considered usage scenarios comprise such situations as identifying and tracking of vehicles which can be used for criminal activities. In an exemplary situation such a vehicle would be tracked and stopped only after it leaves highly populated areas. Another example of application could be searching for lost persons in large uninhabited areas such as forests or mountains.

The INDECT UAV carries a weight of responsibility and if used improperly or by unauthorized personnel it could cause some damage. The major threats could be:

- sending the UAV in flight restricted area and ignoring all warning messages could cause the UAV to a collision. This threat is being minimized by developing a collision evasion system.
- the UAV could be sent into a mission without appropriate permissions thus violating personal privacy

INDECT takes into consideration potential threats related to UAV units. Measures are being taken into consideration in order to prevent and react to potential malfunctions. An example can be parachutes which can be automatically deployed in case of dangerous situation.

City Sensor Network

We believe that the City Sensor Network carries no serious threats since its purpose is to forward encrypt information from various nodes. However if it would be hacked by someone the information could be eavesdropped, deciphered and used in ill manner. The time needed to do this and the usefulness of the information (it changes rapidly, so its lifespan is measured in minutes because the information is overridden by the new ones) makes this case very improbable.

Tracking devices

The risk of improper use of tracking devices is very limited. In order to use it in the wrong way someone would have to hack into the command centre and have physical access to the device at the same time.

Also the police officers responsible for planting the device could place them without appropriate permission and/or warrant.

Measures to be undertaken comprise multiple login to the system (2 or more authorising persons would be required in order to have access to information coming from tracking). All events related to the usage of the tool (including persons having access to such tool) would be monitored and logged.

Plate recognition system

Vehicle plate recognition is a sensitive problem. Improper use of the plate recognition system could only be done by someone having access to the command centre or after hacking into the infrastructure. Because this system supports finding cars with specific plate numbers someone wishing to steal a specific car could have the information where this car has been seen last or what is its usual path.

There is also a threat that police officers responsible for this system would use this system without appropriate permission to search for their own purposes.

Measures to be taken are similar as in the previous case.

Blue force tracking

In hypothetical scenario someone who hacks into the infrastructure or has access to the command centre could have the information where are specific police cars thus enabling

planning a bank job, heist etc. Such scenario is highly improbable taking into account existing and planned systems for protecting information.

4.3 Work-Package 3 – Intelligent integrated agent-based system supporting observation, analysis and detection of criminal activities and threats in complex real-virtual environments

The main goal of WP3 is to utilize the software MAS (Multi-Agent System) approach to develop an information system for analysis and detection of serious criminal activities and threats. The system is dedicated to support the operational activities of the Police, including widely used by the Police techniques of criminal analysis. The functionality of the system will cover analysis of data from different sources, searching for specific information on the Internet, as well as Botnet detection and confinement.

This Work-Package will create MAS (Multi Agent System), an agent-based information system for observation, analysis and detection of criminal activities and threats. The system will include analysis of data sources, support for criminal analysis (detection of roles based on Social Network Approach, visualization of complex relationships), monitoring and detecting illegal content on the Internet as well as Botnet detection and confinement. Criminal analysis is a complex process involving: importing external massive data coming from different sources and in various formats, data analysis such as filtering, frequent patterns searching, statistics as well as data visualization using different types of diagrams (ex. schema, timeline, map) and charts which allows for testing and proving hypotheses. To support this process (with all above stages) – the LINK tool will be provided.

Potential threats, which can arise as an effect of the unauthorized use of the system, are subject to accessibility of the sources of information which is processed. The problem of retention and use of this information during operational and proof procedures is a matter of regulations that the Police is obliged to follow.

The traffic capturing tools being developed to be employed for Lawful Interception (LI) purposes may be susceptible of misuse. Therefore, it is necessary to address this potential threat to the privacy of European citizens by different means, both procedural and technical ones.

First of all, in order to monitor the traffic of a suspect it is necessary, not only to have a traffic capturing tool, but also to have physical access to tap the communications link (e.g. ADSL). Therefore traffic capture for Lawful Interception can only be performed by Security Forces in cooperation with the Internet Service Provider (ISP) of the person subject to an appropriate Wiretap Warrant. The authority that is entitled to issue such wiretap warrants depends on the legislation of each European country, usually a judge or a senior police officer.

Moreover, the INDECT Lawful Interception tool will feature different technical mechanisms to avoid its misuse by third parties or even unauthorized police officers. In particular, both the capturing station and the analysis server can only be activated by means of a Digital Wiretap Warrant (DWW), which is also issued by the authority that provides the legal Wiretap Warrant. Thus, the capture station will only run if a Digital Wiretap Warrant, digitally signed by the appropriate authority, is present. Moreover, the capture file will be encrypted and signed by the capture station. Therefore, the Lawful Interception analysis module will only be able to process such data if the same Digital Wiretap Warrant is in place. Finally the

visualization module implements an access control mechanism that avoids unauthorized users to access captured data, and securely logs all accesses from authorized users.

4.4 Work-Package 4 – Extraction of Information for Crime Prevention by Combining Web Derived Knowledge and Unstructured Data

This Work-Package will provide tools for Relationship Mining. The input will be text from forums, blogs & social networks. The output will be provided as: identification of criminals, criminal organizations and other named entities, identification of relations between entities as well as identification of events in which entities participate. As an input, textual description of solved crimes will be provided. Then, the learning process will start, modelling criminal behaviour patterns. Finally, as an output, prediction of characteristics of offenders will be proposed for unsolved cases.
Tools elaborated in this Work-Package can be employed for identification of encoded information used by criminals (drug dealers, paedophiles, dealers of human organs, etc.). Final outcome would be identification of specific servers. Further proceedings would consist of regular police and prosecutor's procedures accordingly to existing regulations in European Union.

The software produced in WP4 has potential of dual use or misuse. WP4 will produce general purpose natural language understanding software that will interpret entities (persons, locations, dates, organisations etc.) and their relationships. The software produced within WP4 has multiple uses such semantic search (e.g. finding out the companies Microsoft bought in the last 2 years), person search (e.g. find out the current location of 'John Smith who used to work for IBM in 2005'), scientific research (e.g. find out the current drug trials for malaria). It also has potential misuse or dual use. For example, collecting all publicly available information regarding a person. Monitoring a single person or organisation of all its activities that have been reported in the internet. However, it has to be noted that WP4 can only be employed to analyse a data source that has been either provided to the software or available publicly on the Internet.

Reporting of usage of such system will allow for monitoring activities related to the usage, persons having access to the tool and results of the search.

4.5 Work-Package 5 – Search Engine for Fast Detection of Person and Documents Based on Watermarking and Agent Technology

Work-Package 5 will provide mainly tools for combating child pornography. One of the main outcomes will be INACT (INDECT Advanced Image Catalogue Tool). INACT will be composed of two utilities: INACT Indexer and INACT Searcher. Using INACT Indexer, Police Officers will be able to convert child pornography evidence files into hash database. Using INACT Searcher and previously generated has database, suspect file systems of individual, arrested computers, can be searched for similar/identical images (proofs).
Another WP5 tool, Multimedia INDECT Crawler – INCR, will support crawling of public Internet resources, with the aim of combating not only Internet child pornography, but also other serious crimes. The application scenario assumes that (i) user provides an address (set of addresses) to the crawler, (ii) images are automatically retrieved from the website for a given depth, (iii) images are analysed in search for patterns, and finally (iv) the user receives the list of the pages with detected patterns.

Similarly to Work-Package 4 also in this case the result would be identification of specific servers related to serious criminal activities. Further proceedings would consist of regular police and prosecutor's procedures accordingly to existing regulations in European Union.

WP5 will also develop face-recognition-based search engine. The objective is a search system engine that is dedicated for searching criminals. According to the usage scenarios it is aiming to lawful face recognition in relation to the concerned person who had committed a serious offence, e.g. involving violence or with a racial/religious motivation. The system is based on face recognition with many features. Verification can be based on mug shots, i.e. using normal face photos, the system will be verified against ability to search in mug shots database. Faces detection in photos from monitoring cameras, Internet, etc., as well as recognition of detected faces in the mug shots databases is considered. Finally searching for criminals in community portals (e.g. public resources of Facebook) using photo of that criminal is planned.

Tools elaborated within Work-Package 5 can play an auxiliary role with tools developed in the scope of Work-Package 4 especially as concerns protection of personal data.

Multimedia Internet Crawling Software (INCR) assists WP4 in the semantic search and watermarking search, simultaneously protecting personal data. Nevertheless, INCR can be potentially misused. Instead of searching for criminals, one may imagine massive feeding the software with pictures (presenting faces) coming from central/government data bases such as police database or border control system. Therefore the access to the crawling tool should be restricted in order to make it accessible only to persons who are in charge of investigations. The access attempts and crawling requests should be logged in order to be able to detect unauthorised access and usage attempts. All the communication with the crawler tool should be secured, in order to protect the confidentiality of the investigation.

Furthermore, **INDECT Advanced Image Catalogue Tool (INACT) local data repositories** could also get misused. One may imagine counterfeiting the local data repository of forbidden content, and then, recording non-criminal users' private computer activities. Therefore, even if most of the tasks performed on the local data repositories are done off-line within the police premises, the database of forbidden content created by the software tool should be encrypted for added protection. Please note; however, that the internal police procedures for the access limitation and controlling are out of scope of the project.

Face recognition module could also get misused. Therefore the access to recognition module should be limited and logged. Every access to the database should be registered similarly as it is done for prosecutor's files. The system should also provide high security level for confidential personal data, as it is used for access to the prosecution file.
It should be kept in mind that the face search will be dedicated to persons having a serious police records and not to citizens as the whole.

Finally, the developed **digital watermarking techniques** could get misused as well. Individuals or private companies could use watermarking for hiding forbidden messages or criminal content as well as for flagging content to ease monitoring its reuse on the Internet. Other dual use applications could include protection and disclosure of forbidden, criminal content using content watermarking-based access protection algorithms as well as imposing own digital watermarks into images in order to counterfeit their authorship. Anyway, the main end-user of INDECT solutions is police forces. Consequently, there is no direct way of

private, dual-use of digital watermarking solutions. Nevertheless, this is technologically possible, and if ever happens – only outside the INDECT project framework. It should be stressed however that the main objective of using watermarking techniques is for protecting personal images and other data that can be uses for identification such as vehicle number plates.

4.6 Work-Package 6 – Interactive Multimedia Applications Portal for Intelligent Observation System

Work-Package 6 will deliver INDECT Web Portal which will provides a single point of access' to various INDECT tools ("intelligence subsystems") coming not only from WP6 but also from other WPs (integrating and offering some of the INDECT functionalities). Heterogeneous data will be arranged into cases represented by online-available workspaces folders. Cases will contain text, pictures, multimedia (e.g. a description of a criminal on the photo or a web page snapshot with a nickname, etc.). Response will be personalized according to the user profile (e.g. role, privileges, etc.). The Portal will offer video-call management as well. Functionality of the Portal will support the activities of the Police in the field of crisis management, according to predefined police procedures based on the specially created for that purpose workflow. Workflows identify in a clear way the process of transmission of decisions and information flow at various levels of a conducted operation. Workflows will also reduce the risk of incorrect decisions by coordinating the usage of IT services needed for a given task and reflecting different 'roles' of officers while conducting among other actions in the field of crisis management. Visual software will allow non-programmers to edit workflows what will increase system flexibility and reduce maintenance costs.

This analysis considers the possibility of using the WP research results for purposes contrary to their objectives including Dual Use and others.

WP6 Main goals

The main goals comprise the design and implementation of an integrated intelligent portal with functionalities such as the acquisition of heterogeneous data, and its role-based data/user verification. The real-time operation and multimedia communication involved in the transmission of the data. The centralization of decision making using these tools and the higher level processing visualisation of the monitoring process that will present the different types of information available from urban areas concerning threats in real and virtual environments. This includes the management and maintenance of the resulting integrated system.

Portal Functionalities:

The Portal is an end user's entry point for different INDECT functionalities and semantically integrating the services provided by different INDECT subsystems. It includes the storage, access, processing and exchange of different types of data taking into account the security requirements.

In addition the WP will propose workflow and document management support that considers end users' daily duties in crisis situations.

Main attack points:

The way to exploit the INDECT project results by an attacker could be:

- By using the knowledge of the technology components developed as a separated level on which to base attack decisions.

- By using the same technology, unlawful agencies could emulate the security set up of the security forces to implement their own security architecture. This would be the main dual use risk for WP6 that offers a limited possibility of success for the attacker as access to the fully tested implementation will be very hard to get by. Nevertheless INDECT ideas could be implemented for the purposes of an evil organization but this would require the duplication of most of the detailed work on the Portal

- Based on the knowledge of the architecture, flows etc. It could implement the corresponding countermeasures to block the action of the lawful security elements. For example knowledge of the workflow used by the Police the rogue agents could design strategies that take advantage of the loopholes in the lawful security processes.

For the last element the unlawful rogue would try to achieve access to the databases, the image flows and the planned workflow of the security services based on the knowledge of the architecture and of the individual solutions implemented in the Portal. If the attacker is successful s/he will gain useful information for putting at risk the operations of the security services.

The entry point for an attacker to this Network will be the availability of technical information describing the technical infrastructure.

The knowledge of the technology in itself that has been analyzed and validated for the use in the portal will not provide specific advantages to the attacker. These technologies are going to be as much as possible open technologies in order to take advantage of the evolution and progress of the market. The attacker could find the technical details of the implemented portal solutions in the open standards freely available in Internet.

Nevertheless if the attacker has no specific knowledge of the battery of solutions and protections implemented he will have to spend considerable effort to overcome them. The solutions proposed will allow maintaining the system in a good state of readiness, watching over password management, detecting rogue access, containing access through the proper authorisations and taking into account when giving access the real needs of the user and the structure of the information. It is important to implement contention measurements and tracing tools that will allow post-mortem analysis to identify hidden problems and implement good practices.

4.7 Work-Package 7 – Biometrics and Intelligent Methods for Extraction and Supplying Security Information

This Work-Package will provide tools for biometrics and intelligent methods for extraction and supplying security information. Research will target on event detection algorithms for automatic recognition of threats, like traffic or crowed interactions as well as automatic recognition of biometrics, including visual and sound features. For recognition of criminalists, tools will be provided for offenders detection, movement detection, and finally tracking. The main task of the software is the identification of characteristic features of the followed object, computing of its speed vector, detecting of a presence of people in closed areas, crowd observation, and finally controlling position of the camera to hold the followed object close to

the centre of the screen. This will result in algorithms for people localization in video sequences.
Moreover, tools for gait recognition will be developed as criminals can be identified by gait recognition. There will be two approaches to gait recognition presented: holistic/silhouette and model based. Each approach requires silhouette extraction. Depending of chosen approach the silhouette will be utilized in various ways. In case of model based the silhouette will be partially approximated by lines.
Other tools being developed by WP7 are face and iris location and recognition as well as real-time stereovision tools.
Finally, integration platform for all WP7 research results will be presented. The platform will visualize all relevant information like: area around the monitored site (e.g. traffic information around a stadium), status information of appointed forces, timeline of the event, archive of actions, detailed reports from operating units (e.g. red cross, police or event agency), sorted information from database or internet about the event, video picture with automatic detected scene (e.g. of riot on stadium station), plan of camera positions (e.g. in the station), camera control panel as well as database with monitored points of interest around the stadium.

The prototypes of WP7 as research results are designed to serve police officers and security institutions, working under national and international laws. With respect to the potential dual use of these results, the partners of WP7 do not think that the technology developed in WP7 could be directly applied to military users. The only issue here is unwanted access and misuse by illegal users of legal installations. The partners in WP7 will provide several measures for preventing a misuse or even malfunction of the prototype.

- The prototype will be physically protected from unauthorized access or use, i.e. only the authorized personnel will be able to access and use it.
- All data flows and interchange within the system will be correctly protected from an unauthorized access through strong encryption and authentication.

Mechanisms to ensure that the prototype as a research result does not fall into unauthorized hands:

- All users had to sign an appropriate agreement and conspiracy statement.
- The prototype will have to be worked out on specially developed hardware devoted to this work, and will be disconnected from any external network.
- All the standard protection methods (server, network etc.) will be applied.
- Cryptographic methods and special rules for access to databases will be implemented.

In case of passing any kind of confidential information (e.g., information gathered during monitoring) from one INDECT partner (e.g. database) to another, a Non-Disclosure Agreement (Annex II of Grant Agreement) will be signed.

INDECT will not recognize the spoken content but only emotions of a person producing sound.

The audio monitoring (according to audio event detection) installation should not be able to recognize the spoken content. It could be categorized as noise monitoring from top of the buildings similar to noise monitoring near airports or any other noise producing factors which are located close to urban areas.

4.8 Work-Package 8 – Security and Privacy Management

Work-Package 8 will ensure appropriate security and privacy management. WP8 overviews the security of the overall INDECT Project and researches advanced security technologies: New Cryptographic algorithms, Quantum Cryptography and Security in Mobile Ad hoc Networks. The most relevant WP8 prototype will be a Federated ID Management System supporting different authentication mechanisms, including: Centralized Authentication (eases security administration by enabling advanced authentication mechanisms, instead of dealing with multiple authentication systems with different features/requirements), Single Sign-On (SSO, enhances user experience – login just once per session – while maintaining security) as well as Digital Certificates & Smart Card support (strong authentication for high-security systems).
Ethical Issues
The project faced several ethical issues related to its potential impact and use. Handling of collected personal data while protecting privacy and confidentiality is of major importance for the project; therefore a specific task monitors on this aspect throughout the project. For this purpose Ethics Board was established which supports the project consortium in examining the societal, political and legal aspects of potential applications (especially dual-use applications), defines and approves the future exploitation plans of the project results, and advises in dissemination and communication strategy of research results to a wider audience.
INDECT project obeys rules concerning ethics and protection of personal data. In particular trials of prototypes are performed based on written confirmation that it has received favourable opinions of the relevant national or local authorities in the country in which the research is to be carried out. Cooperation with DETECTER (Detection Technologies, Counter-Terrorism Ethics, and Human Rights) project has been established for more efficient analysis of ethical issues related to security provisioning technologies. DETECTER Coordinator became a member of INDECT Ethics Board.
A new participant, Professor of Ethics, is about to enter INDECT Ethics Board in order to extend the body with a person with ethical perspective.
Additionally Ms Sadhbh McCarthy, Director at Centre for Irish and European Security, has agreed to be an external expert who will evaluate issues related to Societal Impact of work carried out within INDECT independently from Ethics Board.
Most of project deliverables are public. Exemptions to public disclosure consider cases which contain financial statements or could impact negatively on law enforcement capabilities or business competitiveness.
In order to disseminate results, INDECT Project website has been established under the following address: http://www.indect-project.eu/. The basic functionality is to provide information about the INDECT Project. Furthermore, the Website lists partners, Deliverables, project news, etc. Furthermore, to disseminate results, the annual International IEEE Multimedia Communications, Services and Security conferences are organized, with the participation of researchers from the E.U. and the U.S. The objective is present high-quality scientific publications in the field of INDECT.

Work Package 8 of the INDECT project will only research and develop security technologies, including new Cryptographic Algorithms, Quantum Cryptography (QC) protocols, Federated ID management systems and Secure Routing Protocols for mobile Ad Hoc Networks (MANET). These technologies will help Security Forces to carry out its duty to serve and protect European citizens in a secure way, guaranteeing the privacy of the exchanged information and that it is only accessed by the parties authorized to do so.

5 INDECT Synopsis Clarifying the Actual INDECT Project Research

INDECT aims at developing tools for enhancing security of citizens and protecting confidentiality of recorded and stored information. In INDECT the threats are considered both in virtual and real environments. Furthermore, INDECT elaborates some horizontal technologies.

As far as threats in virtual environment are concerned, INDECT targets Internet child pornography, trafficking in human organs, and spread of botnets, viruses, malware, and others. Furthermore, INDECT will provide tools for identification of criminal organizations, identification of relations between their members as well as identification of events in which they participate.

As far as threats in real environment are concerned, INDECT targets serious crimes, including terrorism threats, as well as missing and endangered people. The goal is acquisition and analysis of audio and video streams from mobile (UAV) and fixed (CCTV) cameras and microphones. The objective is to support operational activities of police officers and other public services with techniques and tools for the observation related to criminal activities. INDECT will provide several tools for privacy protection and anonymity technologies.

As far as horizontal technologies are concerned, INDECT will deliver "a single point of access" to various INDECT tools, offering some of the INDECT functionalities. Furthermore, INDECT will ensure appropriate cryptographic security management.

In order to clarify the uncertainties which have been raised in the Internet lately, we would like to gather and answer them in this section.

5.1 General INDECT Methodology

INDECT is a research project. The list of objectives does not include any kind of global monitoring of any society.

The INDECT methodology imposes:

1. First, detecting specific crimes (like: Internet child pornography, trafficking in human organs, spread of botnets, viruses, malware as well as terrorism and organised crime), and, only then,
2. Second, detecting specific criminals standing behind the detected crimes (http://www.indect-project.eu/files/public-stories/indect-homepage/methodology).

The definitions of "suspicious behaviour" situations to be detected (and their parameters) will be provided by police departments. Police partners define and assess the usability of tools and algorithms developed by researchers for fighting crime and terrorism threats. As regards to the definition of "suspicious behaviour" ("abnormal behaviour"), the term is not introduced by the INDECT Project, and it was created by EC and explained in the FP7 Work Programme. This term will be always controversial. In our case we clearly understand abnormal behaviour as "criminal behaviour", and especially as "behaviour related to terrorist acts, serious criminal activities (e.g.: murders, bank robberies, someone leaving the luggage in the airport with the bomb) or criminal activities in the Internet (e.g.: child pornography)". We will produce the tools to avoid such situations.

As all projects realised in the scope of EU 7th Framework Program INDECT is a subject to periodic reviews. This year the project will undergo a mid-term review. Independent experts will evaluate the work progress of INDECT, compliance of the research performed with objectives defined before the project was accepted for financing.

5.2 Detecting Threats in Real Environment

Our research for the detection of threats by intelligent cameras, especially those threats related to terrorism, can be used by companies producing equipment for monitoring the safety of people at the stadiums during Euro 2012 in Poland and Ukraine.
In the INDECT Work Plan, the INDECT Consortium has stated that "scenarios for proceeding in the event of terrorist threats during European Football Championships 2012 (Euro 2012) in Poland and Ukraine will be prepared as a part of INDECT realisation".
INDECT as a research project will not perform testing of such equipment in the stadiums. We would like to point out that if some of our research on the detection of threats will require some experimental studies, we will conduct these experiments on university campuses.
When doing this, according to the procedures, informed consent from persons involved in the experiments will be collected. The tests are conducted exclusively within the universities and directly adjacent areas, in the wake of obtaining all the possible approvals and permits, from people whose image and voice is recorded and stored.

5.3 Detecting Threats in Virtual Environment

INDECT does not involve the creation of any technology, which uses software tools remotely installed on users' computer systems. Anyway, INDECT researches INACT Content-Based Search System (INDECT Advanced Image Catalogue Tool) in order to target child pornography. INACT consists of two units: INACT Indexer and INACT Searcher. Using INACT Indexer, police officers are able to convert child pornography evidence files into a hash/descriptor database. Using INACT Searcher and the previously generated database, suspect file systems of individual, arrested computers, can be searched for similar/identical images (proofs). "Arrested" – which means put into custody according to the country regulations. For example in Poland the Police in order to do a search of a suspect's computer have to obtain a legal warrant, which is issued only in cases when a justified suspicion of commitment of crime exists. Currently, the first version of INACT demonstrator is being verified by Polish Police. In the next steps the INACT search engine will be developed with respect for more efficient searching.
INDECT will not use highly sensitive material, such as telephone intercept, VoIP, etc. Researchers from the INDECT consortium do not have access to non-public personal information stored in databases.

5.4 Dissemination

All relevant information of the INDECT project has been, is and will continue to be made publicly available on the project's website (http://www.indect-project.eu/). The project makes more than average effort in making the information available.
There are numerous ways of dissemination. For example, project results are presented at conferences, in scientific journals and in standardization activities. Furthermore, in May last year INDECT organised a two days' international conference where project results were presented in details: http://mcss2010.indect-project.eu/. In June this year, INDECT will organise another international conference where current project results will be presented in details: http://mcss2011.indect-project.eu/.
The INDECT Project Consortium certainly agrees that transparency is a prerequisite for clarifying the actual INDECT Project research. It is for exactly this reason that all relevant documents of the INDECT project are publicly available on the project's website (http://www.indect-project.eu/). In order to make project information more user friendly and more complete, INDECT has just revamped and updated its website.
INDECT is funded under the Seventh Framework Programme (FP7); grant agreement 218086, as a "Collaborative Project". INDECT research area is defined by the FP7 call

"Increasing the Security of citizens" (SEC-1). INDECT is one out of 60 EU projects related to security call in the framework of FP7. For all funded under FP7 projects, and their reports, there are dissemination levels that are indicated by one of the following categories:

- PU = Public
- PP = Restricted to other program participants (including the Commission Services).
- RE = Restricted to a group specified by the consortium (including the Commission Services).
- CO = Confidential, only for members of the consortium (including the Commission Services).

The vast majority of FP7 reports (including INDECT deliverables) are "PU" (public). Exemptions to public disclosure consider cases which contain financial statements or could impact negatively on law enforcement capabilities or business competitiveness. FP7 Security Program projects do not contain classified information, but publishing police operational documents means making the police weaker what would be against the idea of increasing security.

5.5 Exploitation

As INDECT is a FP7 research project, its application is completely out-of-scope. The Project INDECT does not create new cameras. The implementation (including cameras) of technologies being developed into operational systems is however not covered by FP7 projects. Furthermore, it remains the responsibility of the authorities of the Member States to use these new technologies, taking into account the right of citizens to the protection of personal data, in particular the principle of proportionality (as stated in Article 16 of the Treaty for the Functioning of the EU). Should Member States intend to use such new technologies within the scope of Union law, they are bound to comply with EU fundamental rights as enshrined in the EU Charter of Fundamental Rights, as well as the European Convention on Human Rights, and to address the processing of personal data on a proper legal basis. We expect that the Member States will weigh all the possible aspects of using such technologies in a way that fully complies with the protection of personal data and other fundamental rights.

5.6 Ethical Issues

We should emphasize, that research in INDECT is not meant to collect or process any personal data without the prior written consent of individuals. Should any personal data of individuals be used during the project, this will be done on the basis of "informed consent" of individuals participating in the tests. INDECT will not make any personal data processed in connection with the project available to third parties. The project will not give any personal data available processed in connection with the project to third parties, unless otherwise agreed with the subjects.

For more details, you may want to consult the project's website: http://www.indect-project.eu/, for example tests, please refer to: http://www.indect-project.eu/events/wp1/car-plate-recognition-tests.

The independent Ethics Review panel of the European Commission made a check of the ethical issues raised by the project. The all steps of the evaluation procedure including expert opinions, hearing procedure, have been passed successfully. Only then the project was selected for financial support.

The Ethics Board supervises the ethical aspects of the project's activities. The Ethics Board ensures strict fulfillment of the EU ethical rules on privacy, data protection, prevention of dual use, etc. The Ethics Board ensures strict fulfillment of the ethical rules set to deal with

privacy, data protection, prevent dual use and guarantee informed consent of users in the project.
If required Ethics Board is entitled to report to the Commission on potential improper use of research results. This requires inter alia that Article 8 of the EU Charter of Fundamental Rights be complied with, which gives everyone the right to the protection of their own personal data. It should be noted that personal data processing is limited by human rights, and voluntary acts are guaranteed on informed consent forms signed by persons whose data is being processed.
Furthermore, we see the Ethics Board being an independent body. The Board does not view its role as ensuring compliance as a minimalist task, solely designed to ensure legal compliance. Rather, it sees its function as broader, including overseeing scientific and societal issues related to the research activities conducted within the project. Ethics Board performs reviews of project Deliverables. The reviews consider such aspects as: indication and assessment of ethics related content of project reports, indication of legal framework relevant to the Deliverables, providing recommendations and proposals for possible implementation of tools elaborated in INDECT.
Moreover, the INDECT Project was a subject to scrutiny carried out by Polish General Inspector of Personal Data Protection (pol. Główny Inspektor Ochrony Danych Osobowych – GIODO). Following the scrutiny a letter was issued by the Office of GIODO signed by The Director of Inspection Department, Mrs Bogusława Pilc. The letter states that the scrutiny that was performed at AGH University of Science and Technology had for the scope compliance with regulations concerning protection of personal data (law from 29th August 1997 on Protection of Personal Data) and regulation of the Minister of Interior Affairs and Administration, dated to 29th April 2004 with respect to processing of personal data and technical and organisational conditions that equipment and information systems used to process personal data should be conformant to. During control, no negative comments were received.
For more details, you may wish to consult the ethics section of the project's website: http://www.indect-project.eu/approach-to-ethical-issues.

5.7 Ethics Board composition

At the very beginning of the project (Jan. 2009), the INDECT Project Coordinator designated an Ethics Board which was accepted by Project Board. The initial composition of the Ethics Board has already included, among others, a human rights lawyer, a professor of law and a professor of human computer interaction. In Dec. 2009, the project has already added a new member, a professor of ethics, as an additional external expert to the project's Ethics Board. Because of the strong emphasis on the ethical issues, on Jan/Feb. 2011 yet another new external member of the Ethics Board joined (a professor of ethics and philosophy).

The Indect Ethical Board has a total of eight members now. Of these eight, three are currently employed by the Police Service of Northern Ireland (PSNI). Two are senior police officers and one is a Human Rights Legal Adviser. The presence of police in the Ethics Board provides an excellent opportunity to ensure that all deliverables produced by Indect are subjected to an examination of the ethical issues they raise. The reasons for this are as follows:

- due to their roles, the members of the Ethics Board are acutely aware of the practical consequences of the application of deliverables
- the presence of police members leads to a more focussed decision and review process as to the issues raised by deliverables

- key aspects of assessing the proportionality of an action is whether it is likely to achieve the intended objective, and whether there are feasible alternatives. Police members of the Ethics Board can give a unique insight into these issues.

The PSNI is generally recognised as having the highest standards of human rights compliance. The accountability regime to which it is subject is the most comprehensive in the European Union. Each and every aspect of its work is assessed against UK and European human rights standards.

It would be inappropriate for the majority of members of the Ethics Board to come from any one discipline. The wider membership of the Indect Ethics Board ensures that this is not the case. The police members help ensure that issues of legal compliance, as well as other ethical issues, are identified and dealt with at the earliest possible opportunity."

6 Conclusions

Deliverable D0.6 presents a summary of ethical issues concerning the work and research results in 2010. Actions undertaken in this respect comprised overview of the project from ethical perspective, contacts with other projects, participation to external events, internal meetings and discussions dedicated to specifying ethical challenges and proposed measures to be taken in order to protect privacy of citizens and human rights.

Experience gained by the project participants and comments received from outside the project allow to indicate the key conclusions:

- The previous 2 years of the project made INDECT researchers significantly more sensitive to ethical aspect of their work and tools elaborated in the project
- Further efforts should be done as concerns dissemination activities and clear presentation of INDECT outcomes to the public
- More attention should be paid to protect elaborated tools from unauthorised use of results they provide.

Document Updates

Version[3]	Date[4]	Updates and Revision History[5]	Author
v20110116	16/01/2011	First version	Jan Derkacz
v20110212	12/02/2011	Completed version based on contributions and comments from Ethics Board Members	All Authors
v20110213	13/02/2011	Corrected completed version	Mikołaj Leszczuk
v20110312	09/03/2011	Reviewer's comments included	Andrzej Dziech

[3] In form of "vYYYYMMDD"; Version number and edition should correspond to the actual document name conventions.
[4] In form of "DD/MM/YYYY"
[5] Attach as appendix document reviews when appropriate; describe also the current status of the document e.g. "released for internal review", "released for comments from partners"