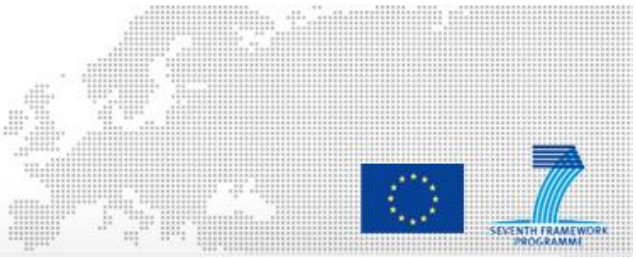
Final Definition of the Evaluation Metrics and Scoreboard for Validation of System Compliance with Privacy

Deliverable 5.1

Lancaster University



Automatic Data relevancy Discrimination for a PRIVacy-sensitive videosurveillance

SEC-2010.6.5-2 - Use of smart surveillance systems, data protection, integrity and sharing information within privacy rules

D5.1 – Final Definition of the Evaluation Metrics and Scoreboard for Validation of System Compliance with Privacy

Due date of deliverable: Month 20

Actual submission date: 12/09/2012

Start of project: 01 February 2011 Duration: 36 Months

Lead Contractor for this deliverable: [lead contractor name]

Revision: [number]

Project co-funded by the European Commission within the Seventh Framework Programme		
Dissemination level		
PU	Public	X
CO	Confidential, only for members of the consortium (including the Commission Services)	

Revision History

Deliverable Administration and summary		
Project Acronym: ADDPRIV	Grant Agreement no: 261653	
Document Identifier: ADDPRIV_20120927_WP5_Lancaster_FinalScoreboard		
Leading partner: University of Lancaster		
Report version: 1		
Report preparation date: 12/09/2012		
Classification: Public		
Nature: Scoreboard		
Author(s) and contributors: Daniel Neyland, Inga Kroener		
Status		Plan
		Draft
		Working
	X	Final
		Submitted
		Approved

The ADDPRIV consortium has addressed all comments received, making changes as necessary. Changes to the document are detailed in the change log table below.

Date	**Edited by**	**Status**	**Changes made**
12/09/2012	Daniel Neyland	Working	First document version
27/09/2012	Anova	Final	

Copyright

Citation

D. Neyland, I. Kroner (2012). Deliverable 5.1 – Final Definition of Evaluation Metrics and Scoreboard for Validation of System Compliance with Privacy. ADDPRIV consortium, www.addpriv.eu

Acknowledgements

The work presented in this document has been conducted in the context of the EU Framework Programme project with Grant Agreement 261653 ADDPRIV (Automatic Data relevancy Discrimination for a PRIVacy-sensitive video surveillance). ADDPRIV is a 36 months project started on February 1st, 2011.

The project consortium is composed by: Anova IT Consulting (ANOVA), Kingston University Higher Education Corporation (KU), Politechnika Gdanska (GDANSK), Lancaster University (ULANCS), Avanzit Tecnologia, S.L. (AVANZIT), Hewlett Packard Italiana Srl (HP), Societá Per Azioni Esercizi Aeroportuali Sea SPA (SEA), Renfe Operadora (RENFE) and The Provost Fellows & Scholars Of The College Of The Holy And Undivided Trinity Of Queen Elizabeth Near Dublin (TCD).

More Information

Public ADDPRIV reports and other information pertaining to the project are available through ADDPRIV public website under www.addpriv.eu

Table of contents

Legal Compliance Scoreboard

The principles in the table below, as well as the legal requirements and questions which follow have been compiled from the various countries national legislation involved in the ADDPRIV project. The EU legislation covering data protection has also been included.

Principle	Legal Compliance	Question
Identifying purposes	Data controller	Who is the data controller?
	Public interest	Defined/not defined? Does this fit appropriate national legislation?
	Clear purpose	Is the purpose of data collection clearly defined?
Openness	Purpose communicated	Communicated/not communicated
Limiting collection	Proportionate application	Proportionate/disproportionate? (Is the collection of data necessary and proportionate to what it seeks to achieve)
	Subsidiary basis	Other means available?
	Minimum intervention	Data only collected for a specific purpose?
	Technological capabilities (proportionate)	Zoom? (Is the zoom function necessary?) Freeze function? (Is the freeze function necessary?) Biometrics? (Is biometric information collected? Is this necessary?)
Limiting use		Is data only used for the specified purpose?
	Private space	Is there an intrusion into private space? Is this necessary?

		Technical remedies?
Accuracy	Accurate and kept up to date	Tested for accuracy? Option for individual to challenge accuracy? Data kept up to date?
Safeguards	Technical measures Organisational measures (physical and administrative)	Security measures in place for access to the control room? Access restrictions? Additional measures? All access logged?
Storage	Period of data retention	Maximum period of data retention in place?
	Secure	Is data stored securely?
Disclosure	Data transfer/copy to third party	Is the data transferred/copied to a third party? Is there a data transfer/copying policy? Is it for commercial purposes? Is it for legal process? Does the transfer contravene the limiting use principle?
	Access to data within the setting	Access control policy? Data adheres to limiting use principle?
Individual access	Right of access	Stored in a way to allow right of access to be exercised?

Challenging compliance	Right to challenge	Individuals have the right to challenge compliance? What are the channels through which individuals can challenge the system? Individuals notified of existence of procedure to challenge compliance?

The above table outlines the legal aspects that a CCTV system must comply with across the UK, Poland, Italy and Spain; incorporating both national and international legislation. The next section of this document moves beyond legal compliance to attempt to develop new ethical standards for surveillance systems in relation to the technology developments proposed within ADDPRIV.

Ethical Compliance Scoreboard

The initial questions within the scoreboard are colour-coded along a traffic light system. A green light highlights little ethical concern or that concerns have been addressed; an orange light highlights some ethical concern to be managed, and a red light highlights an area of major ethical concern that requires attention.

Principles	Questions for analysis		Notes
Risk Assessment	Is there an ongoing risk assessment in place?		Have data flows been mapped? Have risks been identified? Have strategies been put in place for risk management? Will this management be ongoing? How often will a risk assessment take place? Who undertakes the risk assessment? How are they trained? Who oversees the assessor?
Data Collection	Authority to collect personal information?	Yes/No	What is your authority to collect personal information? Has an outside body provided agreement of your right to collect personal information?
	Other means available?	Yes/No	Are other means available to collect the same information?
	Are the goals valid?	Yes/No	Who decides on the goals and their

			validity? Is there an independent body involved in this process (who are they)?
	Does the information cross borders?	Yes/No	What controls are in place? If personal information crosses borders/used for a secondary purpose, is consent required? Is there interconnection to other systems that read the footage? Is there interconnection to other databases? Which ones? What are the access restrictions on these databases?
	Is there a principle of minimisation in place?	Yes/No	Have all options to minimise the routine collection of data been considered? How often are these options assessed?
	Are images pre-loaded?	Yes/No	
	Are there community goals set out (i.e. Does the system benefit the community?)	Yes/No	Who decides on these community goals? Is there an oversight body involved in this process? Is there any community involvement in setting the

			priorities?
	Is there a principle of avoidance of harm in place?	Yes/No	Who decides on the boundaries of the principle? What is included in this? Who oversees the implementation of this principle?
	Does the system impact on third parties (i.e. not the data subject)?	Yes/No	
Use	Authority to use personal information?	Yes/No	What is your authority to use personal information? Is there an external body that has provided authorisation? Who is the external body? Who oversees them?
	Are the uses of the information limited?	Yes/No	Are the uses of the information limited to what a reasonable person might consider appropriate in the circumstances? How is this decided? Is there an external body involved in this decision-making process?
	Are processes automated?	Yes/No	Is human intervention and decision making circumvented? Is this fully, or in part?
	Are there problems with on-going use	Yes/No	Once identified, are 'suspicious'

	of images?		individuals subject to long-term tracking? Are 'suspicious' individuals' images passed onto other security organisations?
	Do uses of the system change over time?	Yes/No	Is there a policy to prevent function creep? Is the policy effective? How is this decided? How often is this policy reviewed? Who by?
	Are there commercial spin offs?	Yes/No	Is this system retained for commercial spin offs? Does the regulation of the system change with these spin offs?

Principles	Questions for analysis		Notes
Communication/ Compliance	Has the data subject been given notice?	Yes/No	Has the data subject been provided with details of the installed surveillance system?
	Is there a right to challenge in place?	Yes/No	How are individuals made aware of this right to challenge?
	Is there covert surveillance taking place?	Yes/No	Any covert surveillance is not acceptable under an ethical system
	Has the data subject provided consent?		Is there a policy that defines consent? Is consent obtained directly from the individual? (If not, why not?) How has consent been obtained? Does consent require an action by the individual, rather than being assumed as the default? Is there a right to refuse data collection in place?
Deletion	Is the obsolete data deleted immediately?	Yes/No	Immediately After 24 hours After 48 hours Kept up to 7 days Kept for longer than 7 days

	What is meant by deletion?		Password protected deleted data? Data removed from the system? Has the route changed? Is it more difficult to get access to the data?
	Are different types of images treated differently?		Are different types of images kept for longer? Are stored images reviewed for deletion? If so, when, and by whom? Are images from different spaces treated differently? Who decides on how different images should be treated?
Results	Is data authenticated?		Are there technical or organisational measures in place to ensure authentification of data?
	False positives? People Objects Actions Route reconstruction	Yes/No	What is an acceptable level of false positives? 0.98 (This is the i-Lids benchmark)[1]

[1] I-Lids is the UK government's benchmark for video based detection systems. http://tna.europarchive.org/20100413151426/scienceandresearch.homeoffice.gov.uk/hosdb/cctv-imaging-technology/i-lids/index.html

	False negatives People Objects Actions Route reconstruction	Yes/No	What is an acceptable rate of false negatives? 0.98 (This is the i-Lids benchmark)[2]
	What is the level of certainty for: Individuals? Objects? Groups?		What is an acceptable level of uncertainty? What is acceptable in terms of third party association (i.e. a non-suspicious individual becomes potentially suspicious)? How are these boundaries decided? Is there an independent body/oversight committee involved in this decision making process?

[2] A rate of 0.98 means that 1 in 50 events would be missed, with 1 in 50 alarms being false.

	How many alerts are there per hour?		What is a manageable number of alerts per hour? What is an acceptable number of alerts per hour? Who decides on what an acceptable number of alerts per hour is? How often is this reviewed?
Storage	Is the data encrypted?	Yes/No	What is the process for encryption? Who has access to the encrypted data?
	Are there levels of access in place?	Yes/No	What is the process by which individuals are authorized to access the system? Password protected? What are the points of access? Is access set to a particular individual? Is access set to a particular action?
	Is there data loss?	Yes/No	Percentage of data loss that is acceptable?: 0% 15% 30% 45%

Accountability	Is there a principle of transparency in place?		Is this principle reviewed? How often and by whom?
	Are there signs to indicate presence of cameras?	Present/absent? Clearly positioned?	Who decides on where these signs should be placed? Is there an independent oversight body involved in the placing of signage?
	Is the controller held to account?	Licensed?	Does the licensing body provide oversight in terms of enforcement?
	Are there contact details provided?	Present/absent? Clearly positioned?	
	What is the positioning of the cameras?	Covert/open?	Covert positioning is not acceptable under an ethical framework
	Accountability to the public? Is there anything that moves beyond 'normal engagement'?		Website Twitter Facebook Rfid Mobile phone app.

	Accountability of the system – is there a system in place?		Who oversees the system? (i.e. data protection officers in each country)? Are the operatives held to account? How? Will there be a lay oversight committee? Will there be independent oversight and certification?
	Is there reflexivity in terms of the system (internal)?		Will there be a CPO responsible for and accountable to on-going running of privacy risk management? Will there be education initiatives? Is there a process for correction of error or redress?
Training	Are there new training programmes in place for the new systems? Are there new codes of practice implemented in line with changes in data protection legislation?		How often are these implemented? By whom? Who oversees the training? Is there an independent body involved in this process?
Crime rates	Does a fall in crime rates justify the implementation of a smart surveillance		Has there been a reduction in crime since the installation of the

	system?		system? How has this been measured?