The Open University

CRISP

CENTRE FOR RESEARCH INTO INFORMATION, SURVEILLANCE & PRIVACY

surprise

"Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe"

Aligning Security and Privacy:

En Route Towards Acceptable Surveillance

Sara Degli Esposti

Centre for Research into Information Surveillance and Privacy (CRISP)

Vincenzo Pavone and Elvira Santiago

Institute of Public Goods and Policies (IPP-CSIC)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

CSIC

Consejo Superior de Investigaciones Científicas

IPP

1. PROJECT GOAL

To understand the reasons behind considering a specific *Surveillance-Orientated Security Technology* (SOST) acceptable.

Rationale: The same measure designed to foster public security might end up increasing public distrust and sense of insecurity.

http://rt.com/usa/nsa-rally-mass-surveillance-786/

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

sara.degliesposti@open.ac.uk

2. METHOD: Surprise Citizen Summit

3 Short Documentary Films

Booklet translated in 8 languages

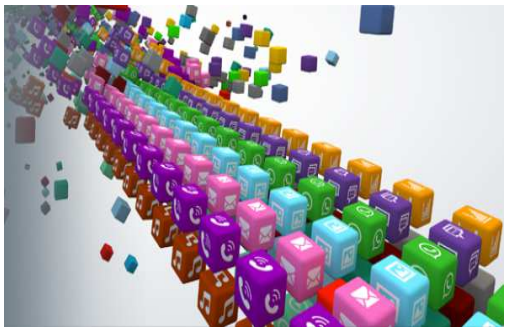
Remote control voting system

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

2. METHOD: 3 concrete SOST examples

Smart CCTV (sCCTV) features digital cameras, which are linked together in a system that can recognise people's faces, analyse their behaviour and detect objects.

Cyber surveillance using **Deep Packet Inspection (DPI)** works by detecting and shaping how messages travel on a network. DPI opens and analyses messages as they travel, identifying those that may pose particular risks



Smartphone location tracking: By analysing location data from a mobile phone, information can be gleaned about the location and movements of the phone user over a period of time.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

2. METHOD: Summits dates & locations

- SLT & sCCTV: Aarhus, Denmark (18/Jan/14); Budapest, Hungary (25/Jan/14); Kiel, Germany (29/Mar/14);
- DPI & SLT: Oslo, Norway (01/Feb/14); Florence, Italy (8/Feb/14); Switzerland (Zürich 8/Mar/14, Iverdu 22/Mar/14, and Lugano 29/Mar/14);
- sCCTV & DPI: Madrid, Spain (01/Feb/14); Vienna, Austria (22/Feb/14); Birmingham, United Kingdom (1/Mar/14 & 15/Mar/14)

Two-SOSTs Research Design

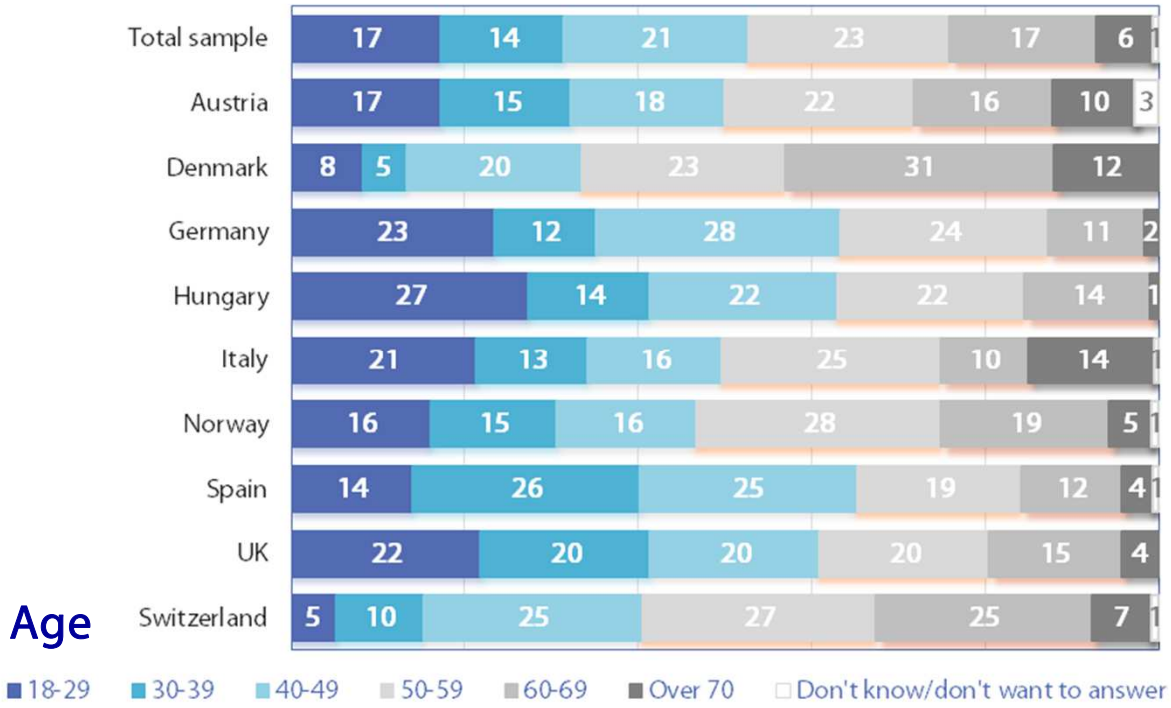
	sCCTV	DPI	SLT
1	Denmark	Norway	Denmark
2	Hungary	Italy	Hungary
3	Spain	Spain	Norway
4	Austria	Austria	Italy
5	UK	UK	Switzerland
6	Germany	Switzerland	Germany
No	1.198	1.202	1.144

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

2. METHOD: Sample composition

A balanced sample in terms of age, gender, education..

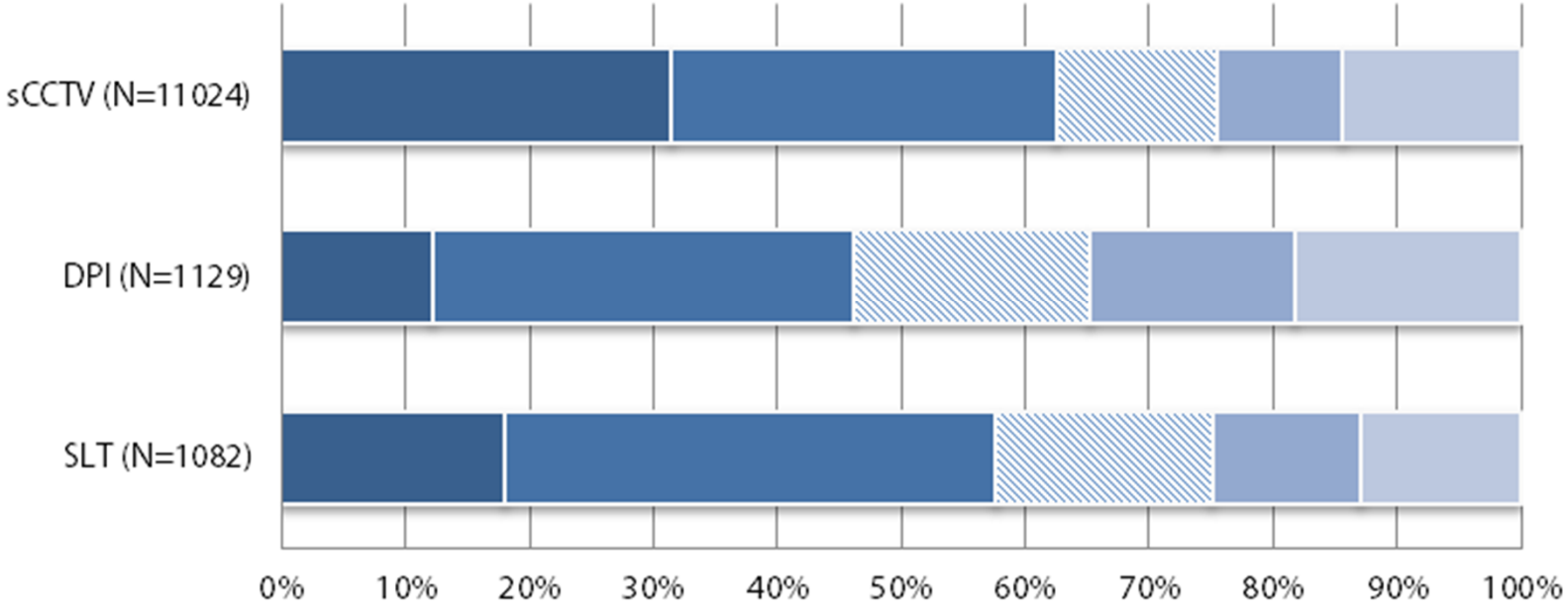
About 200 citizens per country participated in the events



Gender	Austria	Denmark	Germany	Hungary	Italy	Norway	Spain	UK	Switzerland	Total
Female	108	94	117	89	98	61	75	99	142	883
	50,7%	59,9%	63,6%	43,4%	52,7%	54,5%	46,6%	47,4%	58,2%	52,8%
Male	105	63	67	116	88	51	86	110	102	788
	49,3%	40,1%	36,4%	56,6%	47,3%	45,5%	53,4%	52,6%	41,8%	47,2%
Total	**213**	**157**	**184**	**205**	**186**	**112**	**161**	**209**	**244**	1671
	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

3. Theoretical Model

DV1: Overall I support the adoption of sCCTV/DPI/SLT as a national security measure

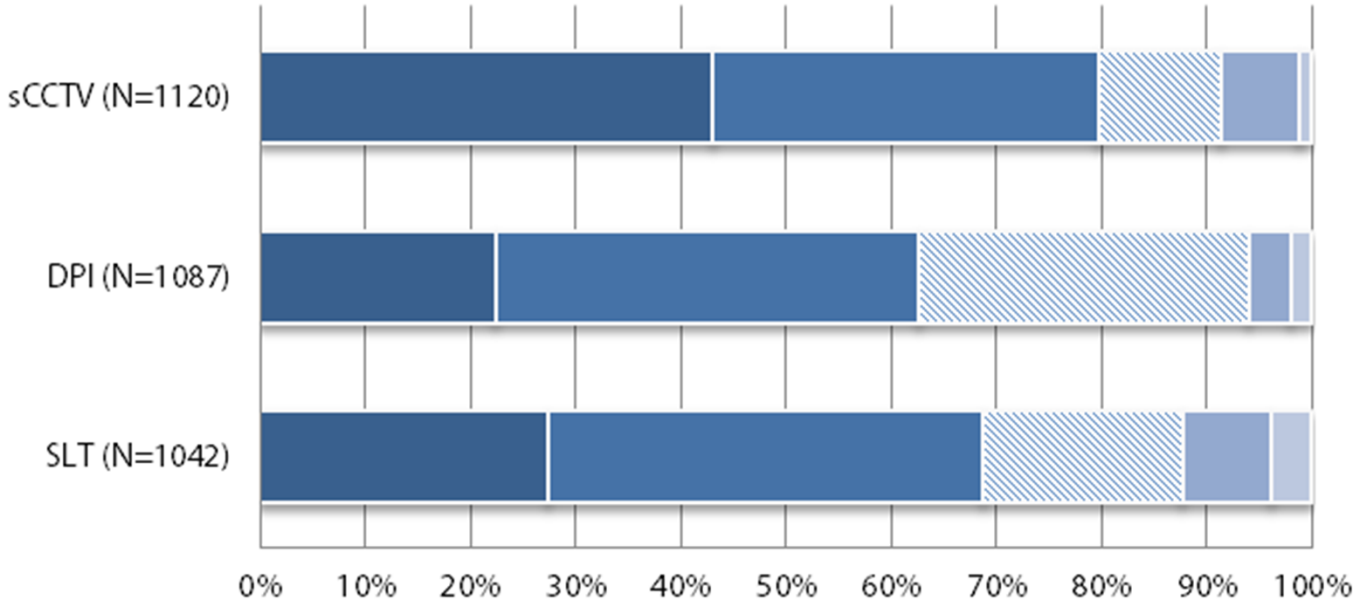


	SLT (N=1082)	DPI (N=1129)	sCCTV (N=11024)
Strongly agree	18,1%	12,2%	31,5%
Agree	39,6%	34,0%	31,0%
Neither agree nor disagree	17,4%	19,1%	12,9%
Disagree	12,0%	16,5%	10,2%
Strongly disagree	12,9%	18,2%	14,3%

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

3. Theoretical Model

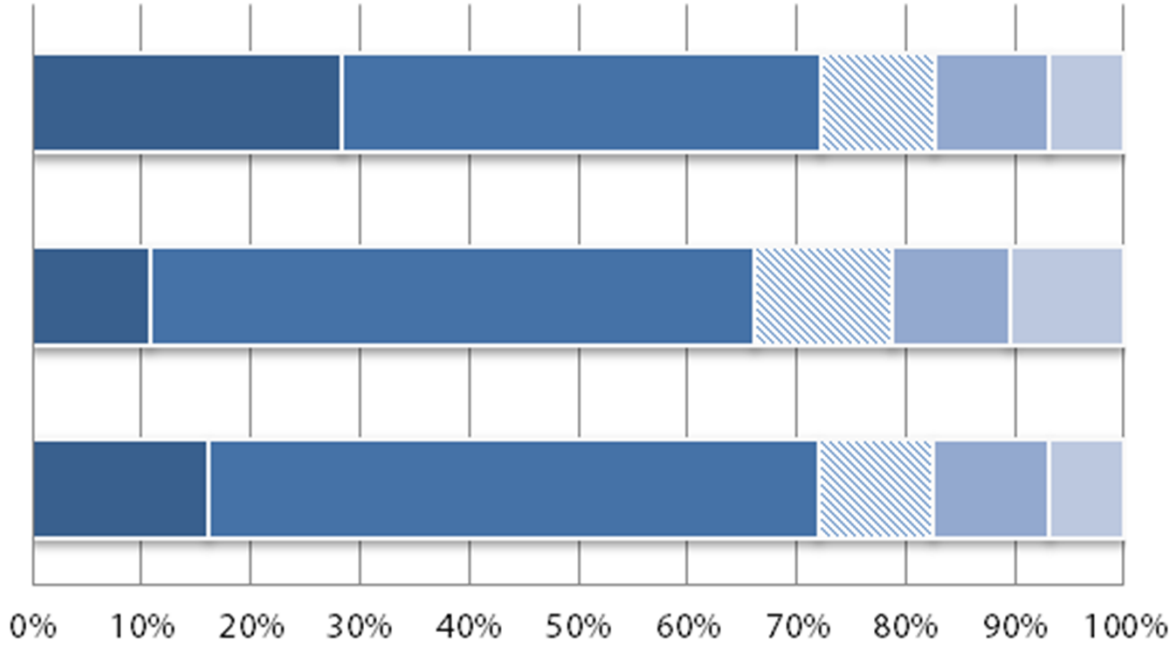
Active avoidance of sCCTV/DPI /SLT



	SLT (N=1042)	DPI (N=1087)	sCCTV (N=1120)
I would definitely not change my behaviour becauseof sCCTV/DPI/SLT	27,4%	22,4%	43,1%
I do not think I would change my behaviour because of sCCTV/DPI/SLT	41,3%	40,3%	36,6%
I would change how I behave because of sCCTV/DPI/SLT	18,9%	31,3%	11,7%
I would avoid going…into areas where sCCTV is used/...online because of DPI/...using a smartphone	8,5%	4,0%	7,4%
I would not go …into areas where sCCTV is used/...online because of DPI/...using a smartphone	3,8%	2,0%	1,2%

3. Theoretical Model

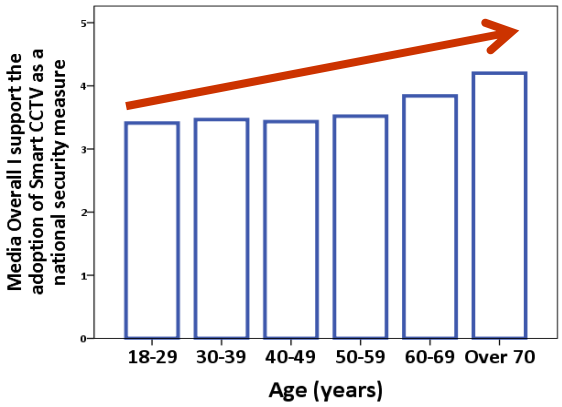
Active opposition toward sCCTV/DPI/ SLT

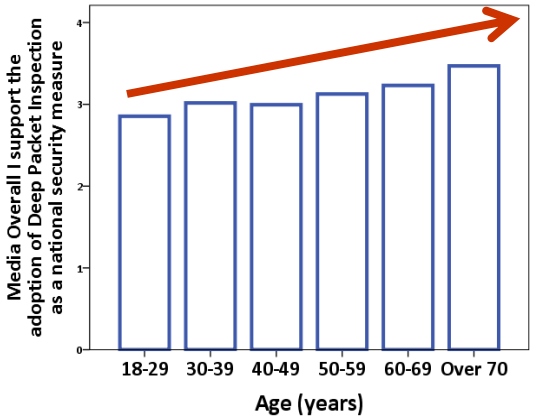


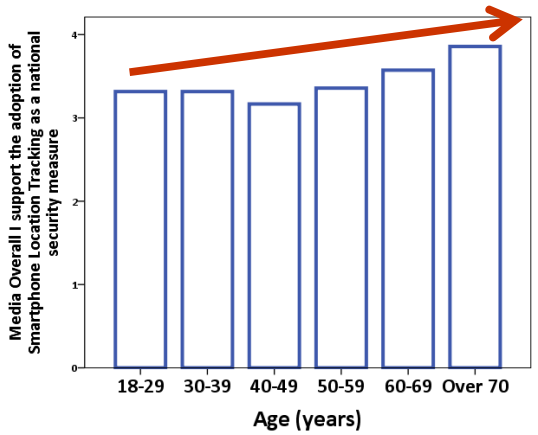
	SLT (N=1050)	DPI (N=1062)	sCCTV (N=1108)
I do not oppose it at all	16,2%	10,8%	28,4%
I would like to find out more how to protect my privacy	55,9%	55,4%	43,9%
I would support others who were protesting against its use	10,5%	12,6%	10,4%
I am prepared to campaign actively against its use	10,7%	10,8%	10,5%
I am prepared to use any means I can to prevent its use	6,8%	10,4%	6,9%

4. RESULTS: Path analysis

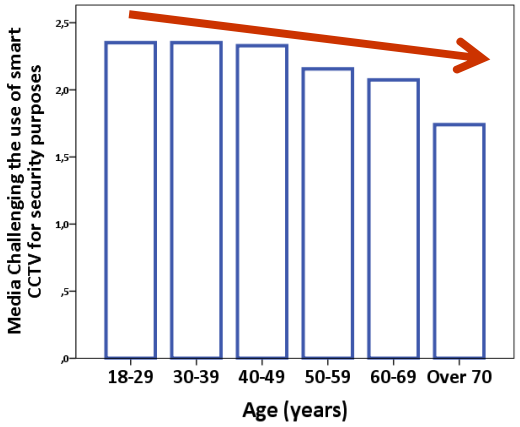
The elderly are less critical…

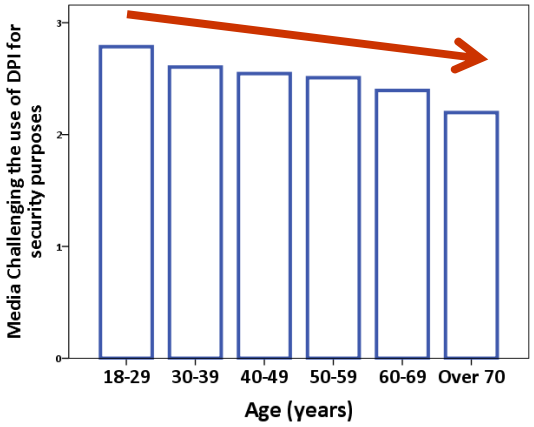


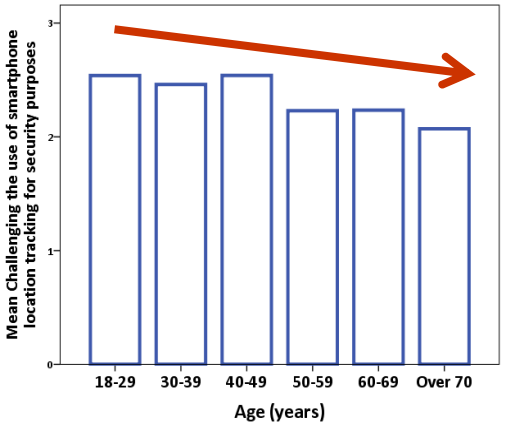




… while young people are those more willing to oppose a new SOST.



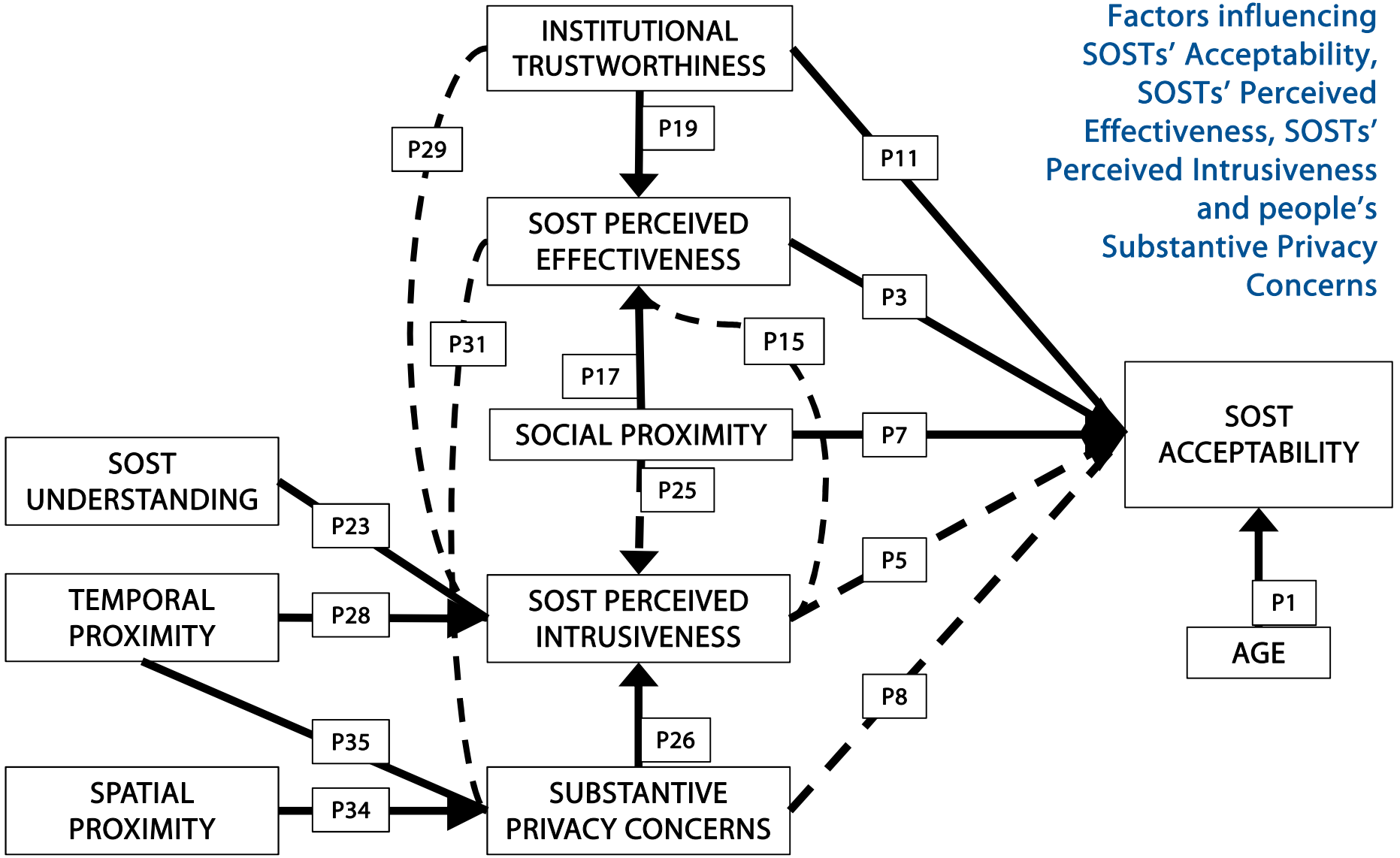




This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

4. RESULTS: Path analysis

Factors influencing SOSTs' Acceptability, SOSTs' Perceived Effectiveness, SOSTs' Perceived Intrusiveness and people's Substantive Privacy Concerns



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

4. RESULTS: Path analysis

ACCEPTABLE SOSTs SHOULD BE …

- … ACCURATE & EFFECTIVE
- … MANAGED BY CAPABLE & HONEST SECURITY AGENTS
- … CLEARLY TARGETED TOWARD CRIMINALS.

SHOULD AVOID TO …

- … PROCESS SENSITIVE INFORMATION ABOUT PEOPLE'S INTIMATE LIVES
- … EXPOSE PEOPLE TO THE RISK OF FEELING EMBARASSED AND SELF CONSCIOUS.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

sara.degliesposti@open.ac.uk

4. RESULTS
Emerging Qualitative Factors

SOSTs which … **Favorable assessment**

✓ … target crimes which are within the citizens' priorities;

✓ … empower citizens and make them feel in control;

✓ … are employed with a clear, delimited purpose in mind.

SOSTs which … **Unfavorable assessment**

× … promote intolerance and segregation;

× … posit high function creep risks;

× … undermine the role of humans;

× … involve private sector or other profit-seeking entities.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

4. RESULTS
Emerging Qualitative Factors

Trustworthiness

- The use of a more acceptable SOST (CCTVs or SLT) helps security agencies to be perceived as more trustworthy. *The key question is not just how safe is the technology, but also* ***how safe is the context*** *in which the technology is implemented.*

Privacy Concerns

- With regards to privacy, **SOSTs which violate one's information privacy (e.g. DPI) are perceived as less acceptable** than SOSTs intruding into one's bodily privacy (e.g. CCTV and SLT). [The internet is misleading perceived as a private space rather than as a public space].

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

4. RESULTS

Does considering SOSTs both as effective and intrusive influence acceptability?

- ✓ **Positive View**: People who consider SOSTs effective and not intrusive are more likely to accept SOSTs.
- ✓ **Trade-off**: People who see SOSTs as both intrusive and effective, are neither more nor less likely to accept SOSTs (except for DPI).

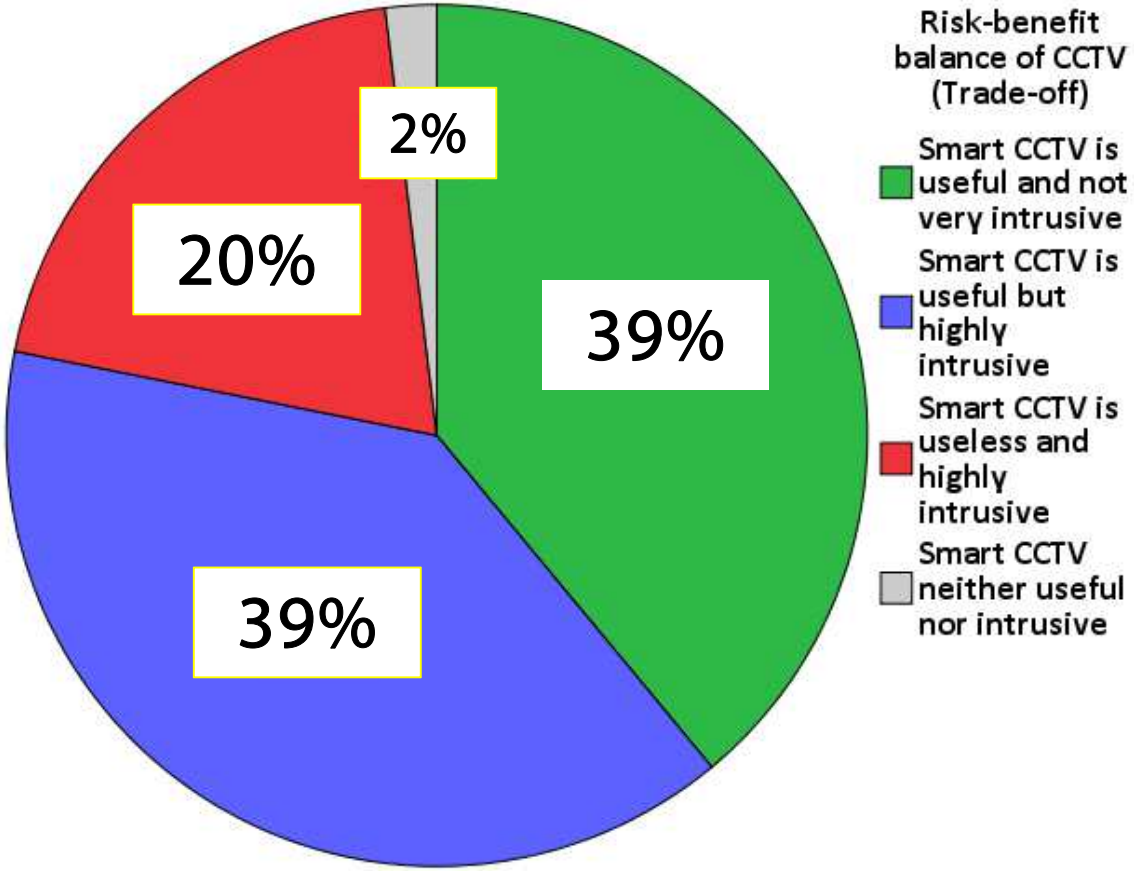
Overall, even those who see SOSTs as both intrusive and effective are **NOT** generally willing to trade privacy in exchange for more security, except for highly controversial SOSTs such as DPI.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

4. RESULTS

sCCTVs: useful and not intrusive?

	Useful	Useless
Highly Intrusive	39,16%	19,95%
Not very intrusive	39,98%	1,92%



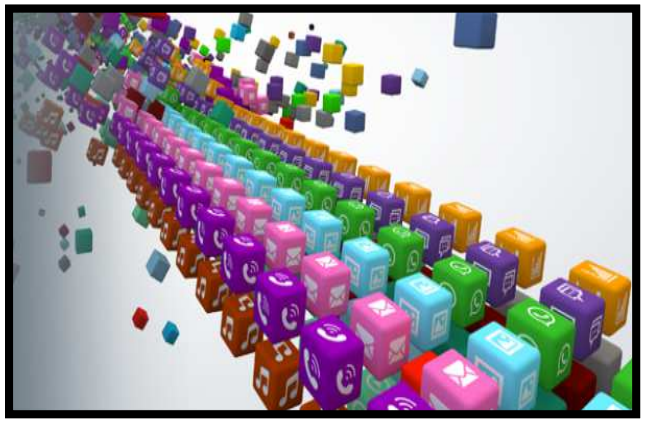
Smart CCTV

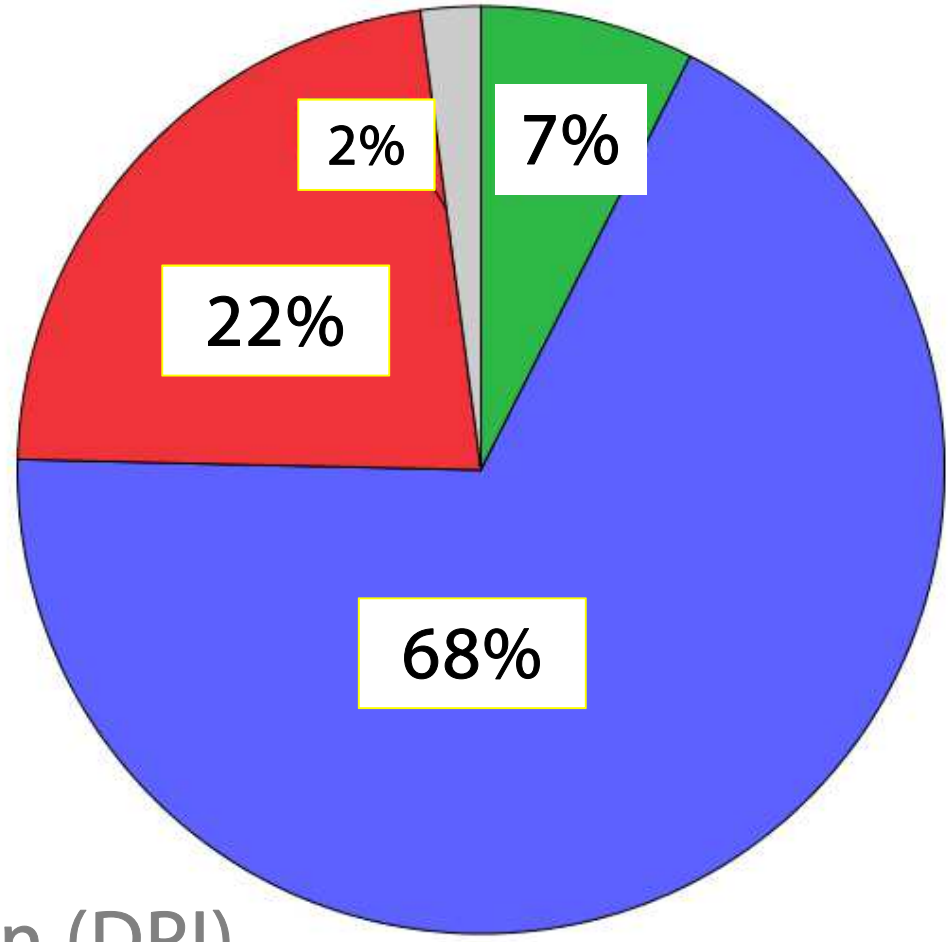
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

4. RESULTS

DPI: useful but highly intrusive?

	Useful	Useless
Highly Intrusive	67,91%	22,55%
Not very intrusive	7,45%	2,02%





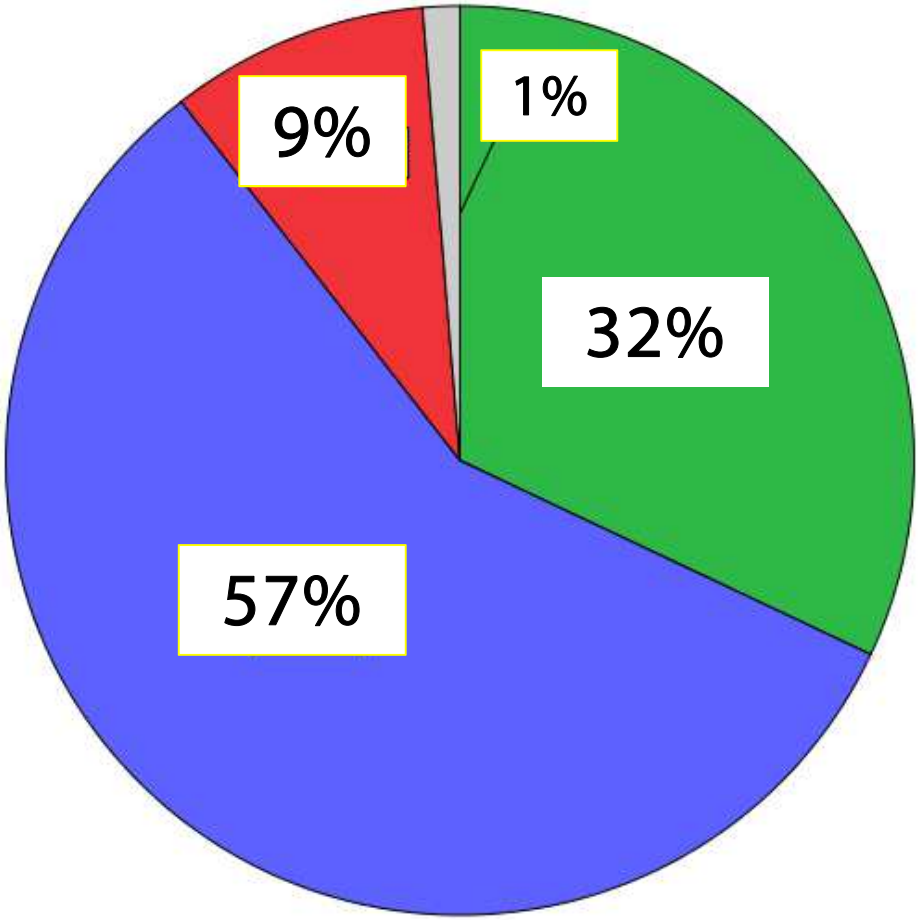
Deep Packet Inspection (DPI)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

4. RESULTS

SLT: effective but highly intrusive?

	Useful	Useless
Highly Intrusive	57,46%	9,2%
Not very intrusive	32,02%	1,31%



Smartphone Location Tracking (SLT)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

Conclusions

- ✓ Acceptable Security Measures—which embed surveillance functionalities—must demonstrate to be able to **foster public safety both in objective** terms, by reducing crime, **and in subjective terms**, by helping people feeling secure and protected.
- ✓ SOSTs should be targeted and should not be part of blanket surveillance strategies. They should be managed by **trustworthy agents** and should **not** make people feel exposed and embarassed.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

sara.degliesposti@open.ac.uk

CRISP
CENTRE FOR RESEARCH INTO INFORMATION, SURVEILLANCE & PRIVACY

The Open University

surprise

MANY THANKS

sara.degliesposti@open.ac.uk - @survgaze
vincenzo.pavone@csic.es
elvira.santiago@csic.es

SURPRISE-PROJECT.EU

IPP

CSIC
Consejo Superior de Investigaciones Científicas

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

Qualitative data supporting and complementing statistical analysis

Trustworthiness

The more trustworthy the security agencies managing a specific SOST are, the more likely to be perceived as acceptable the SOST will be. **The opposite is also true**: the use of a more acceptable SOST (CCTVs or SLT) helps security agencies to be perceived as more trustworthy.

*The key question is not just how safe is the technology, but also **how safe is the context** in which the technology is implemented.*

Privacy Concerns

Participants considered that SOSTs that collect data violating confidentiality of communication, in what are perceived as private spaces, for purposes that are not given priority, are less acceptable. The internet, social media and emails, are perceived as a private space rather than a public space.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

Unexpected factors emerging from qualitative analysis

SOSTs which..

Favorable assessment

✓ ..target crimes which are within the citizens' priorities;

✓ ..empower citizens and make them feel in control;

✓ ..are employed with a clear, delimited purpose in mind.

Unfavorable assessment

× ..promote intolerance and segregation;

× ..posit high function creep risks;

× ..undermine the role of humans;

× ..involve private sector or other profit-oriented entities.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

Distinction between factors and criteria

- FACTOR: something that helps produce or influence a result / one of the things that cause something to happen.
  - Factors can be assessed through both quantitative and qualitative methods
- CRITERION: something that is used as a reason for making a judgment or decision / a standard on which a judgment or decision may be based.
  - Criteria can only be assessed through qualitative methods.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

Criteria adopted by participants to decide on SOSTs' acceptability

1) Public regulatory supervisory body/legislation.

SOSTs are more acceptable when operating within a clear legal framework and under the control of a EU/International regulatory body complementing and transcending national frameworks and national authorities.

2) Transparency, information and accountability

SOSTs are more acceptable if implemented in a context where information is provided to citizens on: a) where SOSTs are used, b) how SOSTs function, c) for what purpose they have been installed and d) who is in charge of managing the system.

3) Public/private separation

SOSTs are more acceptable when operated only by public authorities and for the sake of the public interest. The participation of private actors in security operations makes SOSTs less acceptable.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

Criteria adopted by participants to decide on SOSTs' acceptability

4) Cost-effective

SOSTs are more acceptable when if they offer good value for money. They should be not only effective but also efficient.

5) Data control

SOSTs are more acceptable if they give people control over their data: the right to access, rectify and delete data must be ensured.

6) Data minimization

SOSTs are more acceptable if they keep sensitive data gathering to the minimum, and keep only the information strictly necessary for security purposes. They are more acceptable if they avoid collecting data in spaces considered "sensitive" such as home, private emails or social media.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

Criteria adopted by participants to decide on SOSTs' acceptability

7) Scope and aims of surveillance

SOSTs are more acceptable if they do not operate blanket surveillance, address specific targets, in specific times and spaces and for specific purposes and, when their priorities change, they do so explicitly.

8) Alternatives

SOSTs are more acceptable if they work and operate in combination with non-technological measures and social strategies addressing the social and economic causes of insecurity. SOSTs are more acceptable if they complement and not substitute investments in human resources and social policies.

9) Privacy-by-design

SOSTs are more acceptable if they incorporate and maintain over time privacy-by-design protocols, procedures and mechanisms.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

Q1: Factors influencing acceptance

1) *Institutional Trustworthiness*
    1) Security agents' Ability; Benevolence; Integrity
2) *SOSTs' Perceived Effectiveness*
    1) Accuracy; Perceived Security; Validity
3) *SOSTs' Perceived Intrusiveness*
    1) Risk of Embarrassment; Intrusiveness; Risk of human rights infringement
4) SOSTs' Social, Spatial & Temporal Proximity
5) *Substantive Privacy Concerns*
    1) Intimacy; Anonymity; Solitude
    2) Information Privacy Concerns (Data Collection; Unauthorised Secondary Use; Improper Access; Errors)

Acceptability of

(A) sCCTV

(B) DPI

(C) SLT

Age; Gender; Education; Earnings

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

sara.degliesposti@open.ac.uk

Factors influencing SOST acceptability

Perceived Effectiveness

- *Accuracy*: the extent to which the security measure properly detects and identifies risks or contains error-free records of one's personal information.
- *Perceived security*: the extent to which there is a desirable outcome, as an increase in personal safety, which follows as a result of the introduction of security measure.
- *Validity*: the extent to which the security measure actually addresses a real threat, and uses appropriate data to identify that threat.

Perceived Intrusiveness

- *Risk of embarrassment*: the likelihood that the application of the security measure would lead a person to feel ill-at-ease, uncomfortable, self-conscious or ashamed.
- *Intrusiveness*: the extent to which the security system is forced upon a person without invitation or permission.
- *Risk of human rights infringement*: the extent to which a person believes the security system might violate their human rights.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

Factors influencing SOST acceptability

- *Temporal proximity*, which refers to the extent to which future negative consequences are likely to arise out of the implementation of a given surveillance-based security measure; and,
- *Social proximity*, which refers to the extent to which a given surveillance-based security measure has a well-defined target or whether it treats everyone as potential suspects.

- *Institutional Trustworthiness* refers in fact to the extent to which a particular institution is considered trustworthy, in the sense that it is perceived to be capable of achieving its objectives, concerned about the welfare of citizens and likely to act in good faith.
  - *Ability* – whether the institution is perceived to be able to do what it sets out to do;
  - *Benevolence* – whether the institution is perceived to be concerned about the welfare of citizens;
  - *Integrity* – whether the institution is perceived to act in good faith.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

Factors influencing SOST acceptability

Physical privacy has four dimensions:

- *Intimacy* refers to the integrity of the human body, conceived as encounter of biological tissues and emotional states. It not only reflects the sacredness of the physical self, but also the need of respecting the most intimate relationships, like the ones between lovers, family members or close friends.
- *Solitude* refers to the ability to physically withdraw from social interaction.
- *Anonymity* refers to the possibility of acting without being identified; it represents a way of protecting individual behaviour from collective pressure and others' expectations. The possibility of detaching one's identity from behaviour, or to lose one's identity to be part of a crowd, helps people feel free to make mistakes and express freely their political preferences, such as in the case of democratic elections.
- *Reserve* refers to the capacity of maintaining face-to face communications confidential.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

References

Degli Esposti, S. (2014). "A Roadmap for developing acceptable surveillance-based security measures". *Proceedings of the 9TH Security Research conference »FUTURE SECURITY«*, organised by the *Institutes of Fraunhofer Group for Defense and Security VVS* in Berlin, September 16–18, 2014, pp.71-80.

Pavone, V., Degli Esposti, S., and E. Santiago (2013). SURPRISE FP7 Project: D 2.2 – Draft Report on Key Factors. URL: http://surprise-project.eu/wp-content/uploads/2013/10/SurPRISE-D2.2-Draft-Report-on-Key-Factors.pdf

Pavone, V., and S. Degli Esposti (2012). Public assessment of new surveillance-oriented security technologies: beyond the trade-off between privacy and security. Public Understanding of Science, 21(5), pp. 556-572. URL: http://pus.sagepub.com/content/early/2010/08/23/0963662510376886

Sanquist, T. F., Mahy, H. and F. Morris. (2008). An Exploratory Risk Perception Study of Attitudes Toward Homeland Security Systems, Risk Analysis: An International Journal 28(4), pp. 1125-1133.

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.