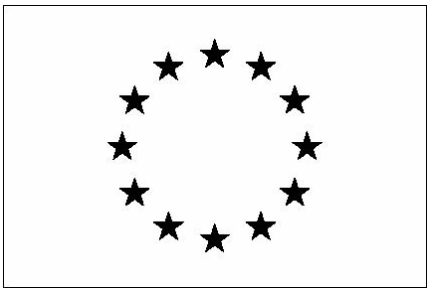

FP7 – SEC- 2011-284725
SURVEILLE

Surveillance: Ethical issues, legal limitations, and efficiency
Collaborative Project

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 284725

SURVEILLE Deliverable D5.10

Report aimed at potential developers, manufacturers and end users on the most common ethical problems encountered in the Advisory Service, offering the advice of the Consortium in the light of the evaluation of the Advisory Service

Due date of deliverable: 31.03.2015
Actual submission date: 30.03.2015

Start date of project: 1.2.2012 Duration: 41 months

SURVEILLE Work Package number and lead: WP5 Prof. Tom Sorell

Author(s):

Dr. Helen McCabe and Dr. John Guelke (UW)

SURVEILLE: Project co-funded by the European Commission within the Seventh Framework Programme		
Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme 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)	

Introduction

This deliverable summarises the advice offered on the six most commonly arising topics in the running of the SURVEILLE Advisory Service. Almost forty discrete topics were raised by users of the Advisory Service (AS), either by the users in their initial set of questions for the AS team, or by the advisors during the course of discussions (for comprehensive list of all topics discussed please see Annex 1). They have been anonymized here to protect the confidentiality of the AS, and all other potentially identifying information has also been removed. Where the topic under discussion is potentially identifying, it has been replaced with 'XXX'.

The deliverable offers brief overviews of key advice offered over the course of the three years of the Advisory Service. The advice is intended to be clear and concise, in order to be as useful as possible to potential developers, manufacturers and end users. However, along with other reporting deliverables D5.8, comprehensively summarizing all of the interactions, and D5.9, evaluating the Advisory Service, the deliverable reflects the UW work in establishing and running the Advisory Service – a significant component of their person months and overall contribution in SURVEILLE.

The most common areas in which advice was sought were regarding data-storage and deletion (thirteen times); dual use (eight times); and informed consent (seven times). Privacy violations, data-sharing and false positives were all raised five times: protection of sensitive data, issues concerning data-controllers, and questions of proportional responses to security issues were each raised four times. Issues that arose three times were collecting/using data without prior consent (e.g. for forensic crime-solving), establishing an ethics advisory board, privacy-by-design, children and recruitment for participation in research. Issues that arose twice were collecting/using data without prior consent (real-time crime prevention), monitoring/using 'open source' data e.g. Twitter, problems of profiling, conflicts with existing EU law, anonymisation, over-wide algorithm categories and encryption.

Data storage was the most inquired after topic by a considerable distance. Questions concerning data storage not only represented a significant fraction of all the topics discussed by itself, but if linked to related topics such as advice concerning data-storage including protecting sensitive data, the responsibilities of data-controllers and questions of data-deletion, advice was sought on the topic twenty-two occasions (the next most prominent topic arose eight times).

Questions to do with what counts as an invasion of privacy, or when invasions might be acceptable, although a significant issue (ranking joint fourth highest), were not a dominant theme of discussion. This in part will reflect the issues that clients were interested in and sought advice about, but in part also represents the previously stated analysis of the SURVEILLE consortium, in particular the views of the ethics partner who had responsibility for running the Advisory Service. This result supports the framework developed throughout WP02 where ethical invasions of privacy were only one of many ethical and legal risks raised

by emerging surveillance technologies.[1] Equally prominent with privacy was the topic of data sharing, each topic arising five times. The third topic to arise five times was that of false positives. This again reflected (an important subset of) an ethical risk identified early in the project – error.[2]

Synthesised Summary of Advice

1. Data Storage and Deletion.

Several clients have been advised to take the questions of data storage and protection, data control and data deletion seriously, and to be aware of their responsibilities as data-controllers. Clients were advised that these latter responsibilities will be spelled-out by the data-control regulations in their specific jurisdictions (and that clients hoping to develop technologies with cross-jurisdictional use will need to consult the laws of each jurisdiction, as well as to bear European law in mind). They were also advised to consult the regulations of their (partner) institutions, or the provider of their research ethics approval. Clients were advised that clearly assigning responsibility for data-control is important for accountability, and were advised (in relevant cases) to ensure that one data-controller be assigned to each work-package, and that they be named on the appropriate consent forms and information sheets.

Regarding safe data-storage, clients were advised about being aware of potential hacking of data, especially by organised crime. In order to minimise these risks, clients were advised to consider ensuring that processing of data is done only by those who already have authority (e.g. the police). In other, non-crime-related cases, clients were advised to consider using encryption in addition to their existing protocols of storing data on local, password-protected computers kept behind locked doors and using anonymising data before sharing it by email. However, it was advised that, in emergency situations (e.g. life-threatening emergencies), encryption should be loosened to aid emergency response.

Clients were also frequently advised on the necessity of timely deletion of data, particularly if they are the data-controllers, and to consider automatic deletion. They were also advised that, in cases where the intended end-user is the police, who are more (legally) accountable, it would be preferable that responsibility for deletion rested with the police, and not with technicians designing the technology or with commercial bodies offering to store data. Clients conducting research on human subjects were also advised that research-participants would need to be told in advance how long their data was going to be stored and when/whether it was going to be deleted. Relevant clients were also advised that, as well as encryption and automatic deletion of data, another way of avoiding risks connected

[1] See in particular SURVEILLE deliverables D2.2, D2.6, D2.8 and D2.9.
[2] Ibid

to data-security was to use less sensitive data to begin with, if possible – e.g. personally-identifying pictures could be pixelated, if collected at all.

2. Dual Use

A number of technologies discussed raised dual use issues. The AS explained to these clients that dual-use issues arise when there is a possibility of misuse, particularly by agents other than those for whom the technology is designed. As one AS summary says, '[d]ual use issues arise when technology intended for one particularly use is used in a different with distinct ethical risks'. This is a wider understanding of 'dual use' than is sometimes recognized by Commission guidance,[3] which often focuses on the military use of civilian technology. In the wider sense of 'dual use' software designed to aid civilian police in the investigation of crime could also help organised crime to avoid successful prosecution or detection. Another distinct ethical risk was that the technology might be used by people for whom it was not originally intended. This might increase the risk of false-positives.

Clients were advised to anticipate possible dual-use issues being questioned by European Commission funders. They were also advised to consider whether privacy-by-design might address some issues of dual-use at the design stage, and that this was always preferably where possible. Relevant clients were also advised, in order to avoid dual-use by human rights abusing jurisdictions, to consider restricting availability by means of export licences.

3. Informed Consent

In the main, advice regarding informed consent took two forms. The first was advice regarding whether informed consent would be necessary for planned research. The second involved the AS approving or suggesting amendments to protocols drafted by clients regarding informed consent (for example, commenting on a proposed information sheet). Clients were also reminded that participants should be offered the opportunity to withdraw their consent (and that if they do, their data should be deleted).

Some specific concerns were raised concerning how properly to administer informed consent in workshops; how to avoid pressurising participants either to participate or to give honest feedback (particularly when asking friends, relatives or members of established networks who might feel pressured to participate and give the feedback they think the research requires); and how to administer informed consent to child-participants.

4. Violations of Privacy

Inquiries about what counted as a violation of privacy arose in various ways. Sometimes clients simply wanted to know if the application of a particular technology represented a violation of privacy and was therefore impermissible, with a number of inquiries centring around the effect on privacy of various kinds of CCTV in public places. Furthermore, the

[3] http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/

privacy of ostensibly 'public' spaces like cafes or restaurants – and analogously open source data from interactions in virtual spaces by means of social networking technology – where nevertheless there is a widespread understanding that norms of privacy operate.[4] Assessing questions like this often required a consideration of the contexts in which incursions on privacy might occur and what these contexts might justify. Life threatening situations justify incursions of privacy that would otherwise be unacceptable. Some technologies are developed specifically for use in life threatening situations, such as emergency response systems (also raising important issues connected with data sharing). Respect for privacy is consistent with acknowledgment that in these contexts normal default assumptions of privacy may be loosened and overridden.

5. Data Sharing

Some questions about data sharing overlapped with questions about privacy, in particular when emergency situations or other threats to life might justify departures from norms appropriate to the everyday context. The ethical permissibility of data sharing will vary greatly on the basis of the purpose for which that sharing takes place – sharing data for the prevention of threats to life or welfare, other things being equal, will be much easier to justify than sharing data for commercial purposes like targeted marketing. The question of who has the legal authority to decide which information can and cannot be shared will also bear on this ethical question, as will the scope of agreements to share information.

Systems for sharing information in emergency situations raise questions about how different kinds of data ought to be categorised. Some kinds of data are more potentially sensitive than others. The Advisory Service has offered suggestions on how data might be categorised for these systems, focussing on which kinds of data is most important for life saving purposes. Similar kinds of sharing systems also arise in relation to so-called 'smart city' applications, outside of an emergency context.[5]

Sometimes the AS suggested technical fixes, like automatic processes to delete data or stop information sharing information once an emergency situation had come to an end. Also in some cases it was recommended that where data was shared among a wider number of people that additional precautions such as anonymisation be taken.

6. False Positives

A persistent risk of much surveillance and surveillance technology is that it may incorrectly identify innocent people as suspect. It is not always an injustice for surveillance to be directed against the innocent. However the consequences of mistakes need to be thought through so that the costs incurred by the innocent are justifiable.

Sometimes the right solution to problems of false positives is an increased role for human judgment – inserting a 'human in the loop'. In some cases for example an algorithm might be oversensitive and cast suspicion too often, and if a human being has to exercise their

[4] The way that privacy norms operate in these different contexts was the subject of SURVEILLE deliverable D4.8, and was also discussed in D4.10.
[5] See also deliverable D4.10.

own judgment before an alarm is triggered this could avoid many unnecessary alarms. However, a 'human in the loop' will not be helpful if they simply defer to the algorithm's categorisation – they have to use their own independent judgment and treat it as more authoritative than the assessment of the technology. For example, smart CCTV that was oversensitive and triggered alerts unnecessarily could be counteracted by good judgment on the part of operators, understanding that their own assessment that an individual is doing nothing significant is more important than any categorisation by the technology.

In other cases the only solution available would be to avoid the use of overly broad categories of behaviour – for example use of extremist symbols or mere mention of keywords -- as a basis for suspicion of violence is unjustified not only because it may be discriminatory or may start to chill legitimate political behaviour and discussion, but simply because it is very likely to generate far more suspects than could ever be usefully followed up on.

Annex 1: Complete list of issues arising in the SURVEILLE Advisory Service

Privacy-By-Design	3
Children	3
Recruitment for participation in research	3
Collecting/using data without prior consent (real-time crime prevention)	2
Monitoring/using 'open source' data e.g. Twitter	2
Problems of profiling	2
Conflicts with existing EU law	2
Anonymisation	2
Over-wide algorithm categories	2
Encryption	2
Use of image-recognition/detection software (to, e.g. identify sex-offenders)	1
XXX	1

Responding to emergency situations	1
Justifiable departures from normal privacy and data-protection norms	1
XXX	1
XXX	1
Collateral damage	1
Deletion of potentially important information (especially regarding smart CCTV)	1
Use of non-lethal weapons	1
Use of video surveillance	1
Media problems	1
Standards governing the use of data for research purposes	1
Use across a range of jurisdictions	1
Research ethics	1

IT ethics	1
Insurance for data-loss	1